chowkidar

Automated Vulnerability Scan Report

chowkidar

Disclaimer

This vulnerability report has been automatically generated using data collected and analyzed by automated vulnerability assessment tools. While these tools are valuable for identifying potential security risks, they have inherent limitations and may produce false positives or overlook complex vulnerabilities that require manual verification.

The purpose of this report is to provide an overview of possible security weaknesses detected within the scanned systems or applications. However, it should not be considered a definitive security assessment. Automated scans do not replace comprehensive manual security reviews, in-depth penetration testing, or risk assessments conducted by security professionals.

Users of this report are strongly advised to conduct independent validation and thorough analysis to confirm the existence, severity, and potential impact of the identified vulnerabilities. Security risks can evolve over time, and the accuracy of this report is limited to the specific conditions and configurations present at the time of scanning.

By using this report, users acknowledge that the findings are based on automated analysis and that additional security assessments are necessary to ensure comprehensive protection. The responsibility for verifying, prioritizing, and remediating vulnerabilities lies with the respective system owners and security teams.

Measurement Scales

CRITICAL - This vulnerability is a high-severity issue with additional security implications that could cause severe business impact. It is classified as critical to emphasize the urgent need for immediate remediation. Examples include risks to human safety, irreversible loss or compromise of business-critical data, or indications of a prior security breach.

HIGH - A high-severity vulnerability presents a significant security risk that could lead to unauthorized access, data breaches, or operational disruptions. While it may not have immediate catastrophic consequences, exploitation could result in major financial, reputational, or regulatory damage. Prompt remediation is strongly recommended.

MEDIUM - A medium-severity vulnerability may not pose an immediate threat but could be exploited under specific conditions to compromise security. Examples include security misconfigurations, exposure of non-sensitive information, or weaknesses that require additional attack vectors to be fully exploited. While the immediate risk may be moderate, timely remediation is recommended to prevent escalation or exploitation in conjunction with other vulnerabilities.

LOW - A low-severity vulnerability represents a minor security weakness with limited impact. While exploitation is unlikely to cause significant harm, resolving these issues can contribute to improved security hygiene and prevent them from being leveraged in combination with other vulnerabilities.

INFO - Informational findings do not represent direct security vulnerabilities but highlight potential areas for improvement or best practice recommendations. These may include system misconfigurations, outdated software, or general security observations that could enhance overall resilience when addressed.

chowkidar

Report Summary

The Report Summary provides a concise overview of key findings, insights, and conclusions from a larger report or analysis. It typically includes a brief introduction, the main objectives or scope of the report, key data points or results, important trends or patterns identified, and any significant recommendations or actions to be taken based on the findings. The purpose of a Report Summary is to quickly inform readers about the essential aspects of the report without having to go through the entire document.

Scope	https://your-scope-url.com
Audit Date	11 Jun 2024
Vulnerabilities Discovered	15

Vulnerability Distribution

Critical	High	Medium	Low	Info
1	2	7	4	1

chowkidar

NO	VULNERABILITY NAME	SEVERITY	CVSS
1	Ports Running Services With Known Vulnerabilities	Critical	9.4
2	Vulnerable To Slowloris DDoS Attack	High	7.5
3	Potentially Vulnerable To SWEET32	High	7.5
4	Missing Security Headers	Medium	6.5
5	Non Compliant TLS Enabled	Medium	6.5
6	No DMARC Record Found	Medium	5.9
7	Vulnerable To Diffie-Hellman Key Exchange Attack	Medium	5.9
8	Vulnerable to Lucky13	Medium	5.6
9	Banner Grabbing	Medium	5.3
10	Directory Listing Enabled	Medium	5.3
11	Potentially Vulnerable To LOGJAM	Low	3.7
12	Review Open Ports	Low	3.7
13	Potentially Vulnerable To BEAST	Low	3.7
14	Vulnerable To Poodle SSLv3 Attack	Low	3.4
15	Endpoints Discovered	Info	0.0

chowkidar

Detailed Vulnerability Report

chowkidar

Ports Running Services With Known Vulnerabilities

Severity	**Critical**
CVSS Score	9.4
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H
CWE	CWE-923: Improper Restriction of Network Ports/Services

Vulnerability Description

Ports running services with known vulnerabilities refers to the situation where network ports on a server or device are running software services with publicly disclosed security vulnerabilities. This type of vulnerability poses significant risks, as attackers can exploit known vulnerabilities in the services to gain unauthorized access, execute arbitrary code, or disrupt services.
Attackers can exploit these vulnerabilities in various ways, including:

- **Remote Code Execution:** Attackers may execute arbitrary code on the server running the vulnerable service, potentially compromising the server and the data it hosts.
- **Data Breach:** Services with known vulnerabilities may allow attackers to access and exfiltrate sensitive data stored on the server, leading to data breaches and privacy violations.
- **Denial of Service (DoS):** Attackers may exploit vulnerabilities to disrupt services and cause downtime, impacting the availability of applications and services.
- **Privilege Escalation:** Attackers may escalate their privileges on the server through vulnerabilities in running services, gaining higher-level access to the server and other connected systems.
- **Malware Distribution:** Attackers may use vulnerable services to distribute malware to users who interact with the server, spreading infections and causing further harm.
- **Man-in-the-Middle Attacks:** Vulnerable services may be exploited to intercept and manipulate data in transit, leading to man-in-the-middle attacks and data integrity issues.

Potential Risk Associated

- **Unauthorized Access:** Attackers can exploit vulnerabilities in services to gain unauthorized access to the server or network, potentially compromising sensitive data and systems.
- **Data Breach:** Known vulnerabilities can be exploited to access, steal, or manipulate sensitive data, such as personally identifiable information (PII), financial data, or intellectual property.
- **Remote Code Execution:** Attackers may execute arbitrary code on the server running the vulnerable service, allowing them to take control of the server and perform malicious actions, such as deploying malware or conducting further attacks.
- **Denial of Service (DoS):** Vulnerable services can be exploited to launch DoS or distributed denial of service (DDoS) attacks, causing service disruptions and making the server or application unavailable to legitimate users.
- **Privilege Escalation:** Attackers can escalate their privileges on the server by exploiting vulnerabilities, gaining access to higher-level functions and other connected systems.
- **Malware Distribution:** Attackers may use vulnerable services as a means to distribute malware, such as ransomware or trojans, to users interacting with the server.
- **Data Integrity Issues:** Attackers may manipulate or alter data passing through the vulnerable services, compromising the integrity and reliability of the data.
- **Compliance Violations:** Failure to address known vulnerabilities in services may result in non-compliance with regulations such as GDPR, HIPAA, or PCI DSS, leading to potential legal and financial penalties.

Evidence (POC)

The following ports are open and running services that are vulnerable and outdated.

chowkidar

21 ftp 1.3.5b

```
  cpe:/a:proftpd:proftpd:1.3.5b:
        SAINT:FD1752E124A72FD3A26EEB9B315E8382  10.0    https://vulners.com/saint/
SAINT:FD1752E124A72FD3A26EEB9B315E8382  *EXPLOIT*
        SAINT:950EB68D408A40399926A4CCAD3CC62E  10.0    https://vulners.com/saint/SAINT:
950EB68D408A40399926A4CCAD3CC62E    *EXPLOIT*
        SAINT:63FB77B9136D48259E4F0D4CDA35E957  10.0    https://vulners.com/saint/SAINT:
63FB77B9136D48259E4F0D4CDA35E957    *EXPLOIT*
        SAINT:1B08F4664C428B180EEC9617B41D9A2C  10.0    https://vulners.com/saint/SAINT:
1B08F4664C428B180EEC9617B41D9A2C    *EXPLOIT*
        PROFTPD_MOD_COPY    10.0    https://vulners.com/canvas/PROFTPD_MOD_COPY *EXPLOIT*
        PRION:CVE-2015-3306 10.0    https://vulners.com/prion/PRION:CVE-2015-3306
        PACKETSTORM:162777  10.0    https://vulners.com/packetstorm/PACKETSTORM:162777  *EXPLOIT*
        PACKETSTORM:132218  10.0    https://vulners.com/packetstorm/PACKETSTORM:132218  *EXPLOIT*
        PACKETSTORM:131567  10.0    https://vulners.com/packetstorm/PACKETSTORM:131567  *EXPLOIT*
        PACKETSTORM:131555  10.0    https://vulners.com/packetstorm/PACKETSTORM:131555  *EXPLOIT*
        PACKETSTORM:131505  10.0    https://vulners.com/packetstorm/PACKETSTORM:131505  *EXPLOIT*
        EDB-ID:49908    10.0    https://vulners.com/exploitdb/EDB-ID:49908  *EXPLOIT*
        CVE-2015-3306   10.0    https://vulners.com/cve/CVE-2015-3306
        1337DAY-ID-36298    10.0    https://vulners.com/zdt/1337DAY-ID-36298    *EXPLOIT*
        1337DAY-ID-23720    10.0    https://vulners.com/zdt/1337DAY-ID-23720    *EXPLOIT*
        1337DAY-ID-23544    10.0    https://vulners.com/zdt/1337DAY-ID-23544    *EXPLOIT*
        CVE-2023-51713  7.5 https://vulners.com/cve/CVE-2023-51713
        CVE-2021-46854  7.5 https://vulners.com/cve/CVE-2021-46854
        CVE-2020-9272   7.5 https://vulners.com/cve/CVE-2020-9272
        CVE-2019-19272  7.5 https://vulners.com/cve/CVE-2019-19272
        CVE-2019-19271  7.5 https://vulners.com/cve/CVE-2019-19271
        CVE-2019-19270  7.5 https://vulners.com/cve/CVE-2019-19270
        CVE-2019-18217  7.5 https://vulners.com/cve/CVE-2019-18217
        CVE-2016-3125   7.5 https://vulners.com/cve/CVE-2016-3125
        CVE-2017-7418   5.5 https://vulners.com/cve/CVE-2017-7418
        SSV:61050   5.0 https://vulners.com/seebug/SSV:61050    *EXPLOIT*
        PRION:CVE-2019-19272    5.0 https://vulners.com/prion/PRION:CVE-2019-19272
        PRION:CVE-2019-19271    5.0 https://vulners.com/prion/PRION:CVE-2019-19271
        PRION:CVE-2019-19270    5.0 https://vulners.com/prion/PRION:CVE-2019-19270
        PRION:CVE-2019-18217    5.0 https://vulners.com/prion/PRION:CVE-2019-18217
        PRION:CVE-2016-3125 5.0 https://vulners.com/prion/PRION:CVE-2016-3125
        CVE-2013-4359   5.0 https://vulners.com/cve/CVE-2013-4359
        PRION:CVE-2017-7418 2.1 https://vulners.com/prion/PRION:CVE-2017-7418
```

22 ssh 5.3

```
  cpe:/a:openbsd:openssh:5.3:
        SSV:78173   7.8 https://vulners.com/seebug/SSV:78173    *EXPLOIT*
        SSV:69983   7.8 https://vulners.com/seebug/SSV:69983    *EXPLOIT*
        PACKETSTORM:98796   7.8 https://vulners.com/packetstorm/PACKETSTORM:98796   *EXPLOIT*
        PACKETSTORM:94556   7.8 https://vulners.com/packetstorm/PACKETSTORM:94556   *EXPLOIT*
        PACKETSTORM:101052  7.8 https://vulners.com/packetstorm/PACKETSTORM:101052  *EXPLOIT*
        EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985    7.8 https://vulners.com/exploitpack/EXPLOITPACK:
71D51B69AA2D3A74753D7A921EE79985    *EXPLOIT*
        EXPLOITPACK:67F6569F63A082199721C069C852BBD7    7.8 https://vulners.com/exploitpack/EXPLOITPACK:
67F6569F63A082199721C069C852BBD7    *EXPLOIT*
        EDB-ID:24450    7.8 https://vulners.com/exploitdb/EDB-ID:24450  *EXPLOIT*
        EDB-ID:15215    7.8 https://vulners.com/exploitdb/EDB-ID:15215  *EXPLOIT*
        PRION:CVE-2010-4478 7.5 https://vulners.com/prion/PRION:CVE-2010-4478
        CVE-2010-4478   7.5 https://vulners.com/cve/CVE-2010-4478
        SSV:60656   5.0 https://vulners.com/seebug/SSV:60656    *EXPLOIT*
        PRION:CVE-2010-5107 5.0 https://vulners.com/prion/PRION:CVE-2010-5107
        CVE-2010-5107   5.0 https://vulners.com/cve/CVE-2010-5107
        SSV:90447   4.6 https://vulners.com/seebug/SSV:90447    *EXPLOIT*
        PRION:CVE-2016-0777 4.0 https://vulners.com/prion/PRION:CVE-2016-0777
        PRION:CVE-2010-4755 4.0 https://vulners.com/prion/PRION:CVE-2010-4755
        CVE-2010-4755   4.0 https://vulners.com/cve/CVE-2010-4755
```

```
        PRION:CVE-2012-0814 3.5 https://vulners.com/prion/PRION:CVE-2012-0814
        PRION:CVE-2011-5000 3.5 https://vulners.com/prion/PRION:CVE-2011-5000
        CVE-2012-0814   3.5 https://vulners.com/cve/CVE-2012-0814
        CVE-2011-5000   3.5 https://vulners.com/cve/CVE-2011-5000
        PRION:CVE-2011-4327 2.1 https://vulners.com/prion/PRION:CVE-2011-4327
        CVE-2011-4327   2.1 https://vulners.com/cve/CVE-2011-4327


53 domain 9.8.2rc1
  cpe:/a:isc:bind:9.8.2rc1:
        CVE-2020-8616   8.6 https://vulners.com/cve/CVE-2020-8616
        CVE-2016-1286   8.6 https://vulners.com/cve/CVE-2016-1286
        CVE-2020-8625   8.1 https://vulners.com/cve/CVE-2020-8625
        SSV:60500   7.8 https://vulners.com/seebug/SSV:60500    *EXPLOIT*
        PRION:CVE-2014-8500 7.8 https://vulners.com/prion/PRION:CVE-2014-8500
        PRION:CVE-2012-5688 7.8 https://vulners.com/prion/PRION:CVE-2012-5688
        PRION:CVE-2012-5166 7.8 https://vulners.com/prion/PRION:CVE-2012-5166
        PRION:CVE-2012-4244 7.8 https://vulners.com/prion/PRION:CVE-2012-4244
        EDB-ID:42121    7.8 https://vulners.com/exploitdb/EDB-ID:42121  *EXPLOIT*
        CVE-2017-3141   7.8 https://vulners.com/cve/CVE-2017-3141
        CVE-2015-4620   7.8 https://vulners.com/cve/CVE-2015-4620
        CVE-2014-8500   7.8 https://vulners.com/cve/CVE-2014-8500
        CVE-2012-5688   7.8 https://vulners.com/cve/CVE-2012-5688
        CVE-2012-5166   7.8 https://vulners.com/cve/CVE-2012-5166
        CVE-2012-4244   7.8 https://vulners.com/cve/CVE-2012-4244
        CVE-2023-3341   7.5 https://vulners.com/cve/CVE-2023-3341
        CVE-2020-8617   7.5 https://vulners.com/cve/CVE-2020-8617
        CVE-2018-5740   7.5 https://vulners.com/cve/CVE-2018-5740
        CVE-2017-3145   7.5 https://vulners.com/cve/CVE-2017-3145
        CVE-2017-3143   7.5 https://vulners.com/cve/CVE-2017-3143
        CVE-2016-9131   7.5 https://vulners.com/cve/CVE-2016-9131
        CVE-2016-8864   7.5 https://vulners.com/cve/CVE-2016-8864
        CVE-2016-2848   7.5 https://vulners.com/cve/CVE-2016-2848
        1337DAY-ID-34485    7.5 https://vulners.com/zdt/1337DAY-ID-34485    *EXPLOIT*
        PRION:CVE-2017-3141 7.2 https://vulners.com/prion/PRION:CVE-2017-3141
        EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    7.2 https://vulners.com/exploitpack/
EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    *EXPLOIT*
        CVE-2015-8461   7.1 https://vulners.com/cve/CVE-2015-8461
        CVE-2016-1285   6.8 https://vulners.com/cve/CVE-2016-1285
        CVE-2013-6230   6.8 https://vulners.com/cve/CVE-2013-6230
        CVE-2020-8622   6.5 https://vulners.com/cve/CVE-2020-8622
        CVE-2016-6170   6.5 https://vulners.com/cve/CVE-2016-6170
        CVE-2017-3136   5.9 https://vulners.com/cve/CVE-2017-3136
        CVE-2013-5661   5.9 https://vulners.com/cve/CVE-2013-5661
        CVE-2015-1349   5.4 https://vulners.com/cve/CVE-2015-1349
        CVE-2022-2795   5.3 https://vulners.com/cve/CVE-2022-2795
        CVE-2021-25219  5.3 https://vulners.com/cve/CVE-2021-25219
        CVE-2017-3142   5.3 https://vulners.com/cve/CVE-2017-3142
        PRION:CVE-2018-5740 5.0 https://vulners.com/prion/PRION:CVE-2018-5740
        PRION:CVE-2017-3145 5.0 https://vulners.com/prion/PRION:CVE-2017-3145
        PRION:CVE-2016-2848 5.0 https://vulners.com/prion/PRION:CVE-2016-2848
        PACKETSTORM:157836  5.0 https://vulners.com/packetstorm/PACKETSTORM:157836  *EXPLOIT*
        FBC03933-7A65-52F3-83F4-4B2253A490B6    5.0 https://vulners.com/githubexploit/
FBC03933-7A65-52F3-83F4-4B2253A490B6    *EXPLOIT*
        PRION:CVE-2017-3143 4.3 https://vulners.com/prion/PRION:CVE-2017-3143
        PRION:CVE-2017-3142 4.3 https://vulners.com/prion/PRION:CVE-2017-3142
        PRION:CVE-2017-3136 4.3 https://vulners.com/prion/PRION:CVE-2017-3136
        PRION:CVE-2021-25214    4.0 https://vulners.com/prion/PRION:CVE-2021-25214
        SSV:61337   2.6 https://vulners.com/seebug/SSV:61337    *EXPLOIT*
        CVE-2014-0591   2.6 https://vulners.com/cve/CVE-2014-0591
        PACKETSTORM:142800  0.0 https://vulners.com/packetstorm/PACKETSTORM:142800  *EXPLOIT*
        1337DAY-ID-27896    0.0 https://vulners.com/zdt/1337DAY-ID-27896    *EXPLOIT*
  cpe:/o:redhat:enterprise_linux:6:
        SSV:93135   10.0    https://vulners.com/seebug/SSV:93135    *EXPLOIT*
```

```
        SSV:89724   10.0    https://vulners.com/seebug/SSV:89724    *EXPLOIT*
        PRION:CVE-2016-5118 10.0    https://vulners.com/prion/PRION:CVE-2016-5118
        PRION:CVE-2016-4448 10.0    https://vulners.com/prion/PRION:CVE-2016-4448
        PRION:CVE-2016-1962 10.0    https://vulners.com/prion/PRION:CVE-2016-1962
        PRION:CVE-2016-1930 10.0    https://vulners.com/prion/PRION:CVE-2016-1930
        PACKETSTORM:165816  10.0    https://vulners.com/packetstorm/PACKETSTORM:165816  *EXPLOIT*
        PACKETSTORM:153278  10.0    https://vulners.com/packetstorm/PACKETSTORM:153278  *EXPLOIT*
        PACKETSTORM:143369  10.0    https://vulners.com/packetstorm/PACKETSTORM:143369  *EXPLOIT*
        OSV:CVE-2022-22954  10.0    https://vulners.com/osv/OSV:CVE-2022-22954
        MSF:AUXILIARY-SCANNER-SMB-SMB_UNINIT_CRED-  10.0    https://vulners.com/metasploit/MSF:AUXILIARY-
SCANNER-SMB-SMB_UNINIT_CRED-    *EXPLOIT*
        EXPLOITPACK:D127040CBAC5DBD24F717F40D86D1AF6    10.0    https://vulners.com/exploitpack/
EXPLOITPACK:D127040CBAC5DBD24F717F40D86D1AF6    *EXPLOIT*
        EXPLOITPACK:069C31B8DD5A351921E96252215466D8    10.0    https://vulners.com/exploitpack/
EXPLOITPACK:069C31B8DD5A351921E96252215466D8    *EXPLOIT*
        EDB-ID:36741    10.0    https://vulners.com/exploitdb/EDB-ID:36741  *EXPLOIT*
        CVE-2015-0240   10.0    https://vulners.com/cve/CVE-2015-0240
        CVE-2014-6601   10.0    https://vulners.com/cve/CVE-2014-6601
        ADOBE_FLASH_METADATA_UAF    10.0    https://vulners.com/canvas/ADOBE_FLASH_METADATA_UAF *EXPLOIT*
        1337DAY-ID-27866    10.0    https://vulners.com/zdt/1337DAY-ID-27866    *EXPLOIT*
        1337DAY-ID-23513    10.0    https://vulners.com/zdt/1337DAY-ID-23513    *EXPLOIT*
        SRC-2022-0005   9.8 https://vulners.com/srcincite/SRC-2022-0005 *EXPLOIT*
        MSF:EXPLOIT-LINUX-HTTP-VMWARE_WORKSPACE_ONE_ACCESS_CVE_2022_22954-  9.8 https://vulners.com/
metasploit/MSF:EXPLOIT-LINUX-HTTP-VMWARE_WORKSPACE_ONE_ACCESS_CVE_2022_22954-   *EXPLOIT*
        FB4E2E7D-EBA0-5AD8-A2C0-6EE27D053537    9.8 https://vulners.com/githubexploit/FB4E2E7D-EBA0-5AD8-
A2C0-6EE27D053537   *EXPLOIT*
        F2545817-7A3F-52E7-ADC5-B775C0DB8082    9.8 https://vulners.com/githubexploit/F2545817-7A3F-52E7-
ADC5-B775C0DB8082   *EXPLOIT*
        F12DF8D7-84BD-522E-A6CA-0413FBDFB48F    9.8 https://vulners.com/githubexploit/F12DF8D7-84BD-522E-
A6CA-0413FBDFB48F   *EXPLOIT*
        EDB-ID:44294    9.8 https://vulners.com/exploitdb/EDB-ID:44294  *EXPLOIT*
        EDB-ID:41042    9.8 https://vulners.com/exploitdb/EDB-ID:41042  *EXPLOIT*
        D8F56B26-C194-5CA0-83FB-D59BC7014E35    9.8 https://vulners.com/githubexploit/D8F56B26-
C194-5CA0-83FB-D59BC7014E35 *EXPLOIT*
        CVE-2020-27846  9.8 https://vulners.com/cve/CVE-2020-27846
        CVE-2018-5096   9.8 https://vulners.com/cve/CVE-2018-5096
        CVE-2018-5095   9.8 https://vulners.com/cve/CVE-2018-5095
        CVE-2018-5091   9.8 https://vulners.com/cve/CVE-2018-5091
        CVE-2017-7802   9.8 https://vulners.com/cve/CVE-2017-7802
        CVE-2017-7801   9.8 https://vulners.com/cve/CVE-2017-7801
        CVE-2017-7800   9.8 https://vulners.com/cve/CVE-2017-7800
        CVE-2017-7793   9.8 https://vulners.com/cve/CVE-2017-7793
        CVE-2017-7792   9.8 https://vulners.com/cve/CVE-2017-7792
        CVE-2017-7786   9.8 https://vulners.com/cve/CVE-2017-7786
        CVE-2017-7785   9.8 https://vulners.com/cve/CVE-2017-7785
        CVE-2017-7751   9.8 https://vulners.com/cve/CVE-2017-7751
        CVE-2017-7750   9.8 https://vulners.com/cve/CVE-2017-7750
        CVE-2017-7749   9.8 https://vulners.com/cve/CVE-2017-7749
        CVE-2017-5472   9.8 https://vulners.com/cve/CVE-2017-5472
        CVE-2017-5470   9.8 https://vulners.com/cve/CVE-2017-5470
        CVE-2017-5469   9.8 https://vulners.com/cve/CVE-2017-5469
        CVE-2017-5464   9.8 https://vulners.com/cve/CVE-2017-5464
        CVE-2017-5460   9.8 https://vulners.com/cve/CVE-2017-5460
        CVE-2017-5446   9.8 https://vulners.com/cve/CVE-2017-5446
        CVE-2017-5443   9.8 https://vulners.com/cve/CVE-2017-5443
        CVE-2017-5442   9.8 https://vulners.com/cve/CVE-2017-5442
        CVE-2017-5441   9.8 https://vulners.com/cve/CVE-2017-5441
        CVE-2017-5440   9.8 https://vulners.com/cve/CVE-2017-5440
        CVE-2017-5439   9.8 https://vulners.com/cve/CVE-2017-5439
        CVE-2017-5438   9.8 https://vulners.com/cve/CVE-2017-5438
        CVE-2017-5435   9.8 https://vulners.com/cve/CVE-2017-5435
        CVE-2017-5433   9.8 https://vulners.com/cve/CVE-2017-5433
        CVE-2017-5432   9.8 https://vulners.com/cve/CVE-2017-5432
        CVE-2017-5410   9.8 https://vulners.com/cve/CVE-2017-5410
```

```
        CVE-2017-5404   9.8 https://vulners.com/cve/CVE-2017-5404
        CVE-2017-5402   9.8 https://vulners.com/cve/CVE-2017-5402
        CVE-2017-5401   9.8 https://vulners.com/cve/CVE-2017-5401
        CVE-2017-5396   9.8 https://vulners.com/cve/CVE-2017-5396
        CVE-2017-5390   9.8 https://vulners.com/cve/CVE-2017-5390
        CVE-2017-5380   9.8 https://vulners.com/cve/CVE-2017-5380
        CVE-2017-5376   9.8 https://vulners.com/cve/CVE-2017-5376
        CVE-2016-9899   9.8 https://vulners.com/cve/CVE-2016-9899
        CVE-2016-9898   9.8 https://vulners.com/cve/CVE-2016-9898
        CVE-2016-9893   9.8 https://vulners.com/cve/CVE-2016-9893
        CVE-2016-0639   9.8 https://vulners.com/cve/CVE-2016-0639
        CVE-2015-4602   9.8 https://vulners.com/cve/CVE-2015-4602
        CE3963DC-4AF7-5738-83F3-067854F4CE3C    9.8 https://vulners.com/githubexploit/
CE3963DC-4AF7-5738-83F3-067854F4CE3C    *EXPLOIT*
        CB8E07F4-50D7-541D-8B3E-749FACA903E3    9.8 https://vulners.com/githubexploit/
CB8E07F4-50D7-541D-8B3E-749FACA903E3    *EXPLOIT*
        B8601FE7-3E95-5AD7-8C4E-05FAB57FBB6D    9.8 https://vulners.com/githubexploit/
B8601FE7-3E95-5AD7-8C4E-05FAB57FBB6D    *EXPLOIT*
        A8AC5191-F5B7-5FE5-8702-B85CC7107869    9.8 https://vulners.com/githubexploit/A8AC5191-
F5B7-5FE5-8702-B85CC7107869 *EXPLOIT*
        A4A3F324-E3F8-5601-A653-3BFEBF5A4F46    9.8 https://vulners.com/githubexploit/A4A3F324-E3F8-5601-
A653-3BFEBF5A4F46   *EXPLOIT*
        979EA51E-E85A-5272-9311-AE6B0A2F756D    9.8 https://vulners.com/githubexploit/979EA51E-
E85A-5272-9311-AE6B0A2F756D *EXPLOIT*
        95C17878-3493-5938-9D11-1C33940763BA    9.8 https://vulners.com/githubexploit/
95C17878-3493-5938-9D11-1C33940763BA    *EXPLOIT*
        7EA5501E-29E8-5542-869F-EE5E061312E6    9.8 https://vulners.com/githubexploit/
7EA5501E-29E8-5542-869F-EE5E061312E6    *EXPLOIT*
        6A61F003-DE4D-520E-AD93-A581E4E22941    9.8 https://vulners.com/githubexploit/6A61F003-DE4D-520E-
AD93-A581E4E22941   *EXPLOIT*
        4AA1550F-CCB9-5943-A14B-C992259F6426    9.8 https://vulners.com/githubexploit/4AA1550F-CCB9-5943-
A14B-C992259F6426   *EXPLOIT*
        49594F88-14A4-5CA9-9202-ABE72435019C    9.8 https://vulners.com/githubexploit/
49594F88-14A4-5CA9-9202-ABE72435019C    *EXPLOIT*
        479D22AB-BE97-51BA-82CC-F8945ED02516    9.8 https://vulners.com/githubexploit/479D22AB-
BE97-51BA-82CC-F8945ED02516 *EXPLOIT*
        1337DAY-ID-37684    9.8 https://vulners.com/zdt/1337DAY-ID-37684    *EXPLOIT*
        0D5F53B0-63C3-52D0-960A-09382DCD6A64    9.8 https://vulners.com/githubexploit/
0D5F53B0-63C3-52D0-960A-09382DCD6A64    *EXPLOIT*
        PRION:CVE-2016-3610 9.3 https://vulners.com/prion/PRION:CVE-2016-3610
        PRION:CVE-2016-3598 9.3 https://vulners.com/prion/PRION:CVE-2016-3598
        PRION:CVE-2016-3587 9.3 https://vulners.com/prion/PRION:CVE-2016-3587
        PRION:CVE-2016-2799 9.3 https://vulners.com/prion/PRION:CVE-2016-2799
        PRION:CVE-2016-2794 9.3 https://vulners.com/prion/PRION:CVE-2016-2794
        PRION:CVE-2016-1935 9.3 https://vulners.com/prion/PRION:CVE-2016-1935
        CVE-2015-0395   9.3 https://vulners.com/cve/CVE-2015-0395
        CVE-2014-2483   9.3 https://vulners.com/cve/CVE-2014-2483
        1337DAY-ID-28302    9.3 https://vulners.com/zdt/1337DAY-ID-28302    *EXPLOIT*
        CVE-2017-7753   9.1 https://vulners.com/cve/CVE-2017-7753
        CVE-2017-5465   9.1 https://vulners.com/cve/CVE-2017-5465
        CVE-2017-5447   9.1 https://vulners.com/cve/CVE-2017-5447
        OSV:CVE-2023-30628  8.8 https://vulners.com/osv/OSV:CVE-2023-30628
        EDB-ID:50691    8.8 https://vulners.com/exploitdb/EDB-ID:50691  *EXPLOIT*
        EDB-ID:49864    8.8 https://vulners.com/exploitdb/EDB-ID:49864  *EXPLOIT*
        EDB-ID:42484    8.8 https://vulners.com/exploitdb/EDB-ID:42484  *EXPLOIT*
        CVE-2020-14339  8.8 https://vulners.com/cve/CVE-2020-14339
        CVE-2019-17024  8.8 https://vulners.com/cve/CVE-2019-17024
        CVE-2018-10928  8.8 https://vulners.com/cve/CVE-2018-10928
        CVE-2018-10926  8.8 https://vulners.com/cve/CVE-2018-10926
        CVE-2017-7798   8.8 https://vulners.com/cve/CVE-2017-7798
        CVE-2017-7752   8.8 https://vulners.com/cve/CVE-2017-7752
        CVE-2017-3106   8.8 https://vulners.com/cve/CVE-2017-3106
        1337DAY-ID-37293    8.8 https://vulners.com/zdt/1337DAY-ID-37293    *EXPLOIT*
        1337DAY-ID-36241    8.8 https://vulners.com/zdt/1337DAY-ID-36241    *EXPLOIT*
```

```
        CVE-2017-5448   8.6 https://vulners.com/cve/CVE-2017-5448
        CVE-2021-3682   8.5 https://vulners.com/cve/CVE-2021-3682
        CVE-2017-7807   8.1 https://vulners.com/cve/CVE-2017-7807
        CVE-2022-2625   8.0 https://vulners.com/cve/CVE-2022-2625
        SAINT:7E62985F7ECA8ECA0E5491AB646D5F88  7.9 https://vulners.com/saint/SAINT:
7E62985F7ECA8ECA0E5491AB646D5F88    *EXPLOIT*
        EXPLOITPACK:82350D3B53640992505E897CCF35E9D8    7.9 https://vulners.com/exploitpack/EXPLOITPACK:
82350D3B53640992505E897CCF35E9D8    *EXPLOIT*
        CVE-2014-3560   7.9 https://vulners.com/cve/CVE-2014-3560
        SMNTC-108801    7.8 https://vulners.com/symantec/SMNTC-108801
        SMNTC-105108    7.8 https://vulners.com/symantec/SMNTC-105108
        PRION:CVE-2016-7039 7.8 https://vulners.com/prion/PRION:CVE-2016-7039
        PRION:CVE-2016-2776 7.8 https://vulners.com/prion/PRION:CVE-2016-2776
        PRION:CVE-2014-3687 7.8 https://vulners.com/prion/PRION:CVE-2014-3687
        PRION:CVE-2014-3673 7.8 https://vulners.com/prion/PRION:CVE-2014-3673
        PACKETSTORM:158990  7.8 https://vulners.com/packetstorm/PACKETSTORM:158990  *EXPLOIT*
        PACKETSTORM:156729  7.8 https://vulners.com/packetstorm/PACKETSTORM:156729  *EXPLOIT*
        PACKETSTORM:154361  7.8 https://vulners.com/packetstorm/PACKETSTORM:154361  *EXPLOIT*
        MSF:EXPLOIT-WINDOWS-LOCAL-MOV_SS-   7.8 https://vulners.com/metasploit/MSF:EXPLOIT-WINDOWS-LOCAL-
MOV_SS- *EXPLOIT*
        F67B1561-9F99-5BDE-8EDF-EA45E59D6039    7.8 https://vulners.com/githubexploit/
F67B1561-9F99-5BDE-8EDF-EA45E59D6039    *EXPLOIT*
        EDB-ID:45024    7.8 https://vulners.com/exploitdb/EDB-ID:45024  *EXPLOIT*
        EDB-ID:44697    7.8 https://vulners.com/exploitdb/EDB-ID:44697  *EXPLOIT*
        EDB-ID:43331    7.8 https://vulners.com/exploitdb/EDB-ID:43331  *EXPLOIT*
        EDB-ID:42887    7.8 https://vulners.com/exploitdb/EDB-ID:42887  *EXPLOIT*
        EDB-ID:42276    7.8 https://vulners.com/exploitdb/EDB-ID:42276  *EXPLOIT*
        EDB-ID:42275    7.8 https://vulners.com/exploitdb/EDB-ID:42275  *EXPLOIT*
        EDB-ID:42274    7.8 https://vulners.com/exploitdb/EDB-ID:42274  *EXPLOIT*
        CVE-2022-32547  7.8 https://vulners.com/cve/CVE-2022-32547
        CVE-2022-32546  7.8 https://vulners.com/cve/CVE-2022-32546
        CVE-2022-32545  7.8 https://vulners.com/cve/CVE-2022-32545
        CVE-2022-0358   7.8 https://vulners.com/cve/CVE-2022-0358
        CVE-2019-10216  7.8 https://vulners.com/cve/CVE-2019-10216
        CVE-2017-1000366    7.8 https://vulners.com/cve/CVE-2017-1000366
        CVE-2017-1000253    7.8 https://vulners.com/cve/CVE-2017-1000253
        PACKETSTORM:162568  7.6 https://vulners.com/packetstorm/PACKETSTORM:162568  *EXPLOIT*
        57A481B6-594E-5AFE-869B-606BECC0CF16    7.6 https://vulners.com/githubexploit/
57A481B6-594E-5AFE-869B-606BECC0CF16    *EXPLOIT*
        SSV:2397    7.5 https://vulners.com/seebug/SSV:2397 *EXPLOIT*
        SMNTC-111341    7.5 https://vulners.com/symantec/SMNTC-111341
        SMNTC-110958    7.5 https://vulners.com/symantec/SMNTC-110958
        SMNTC-110454    7.5 https://vulners.com/symantec/SMNTC-110454
        SMNTC-105952    7.5 https://vulners.com/symantec/SMNTC-105952
        SAINT:BF16620515318B3BFC6F9DACC4FF2748  7.5 https://vulners.com/saint/
SAINT:BF16620515318B3BFC6F9DACC4FF2748  *EXPLOIT*
        SAINT:AD161DA8F25E93FF26B36F6C31115364  7.5 https://vulners.com/saint/
SAINT:AD161DA8F25E93FF26B36F6C31115364  *EXPLOIT*
        PRION:CVE-2016-5408 7.5 https://vulners.com/prion/PRION:CVE-2016-5408
        PRION:CVE-2016-5254 7.5 https://vulners.com/prion/PRION:CVE-2016-5254
        PRION:CVE-2016-2182 7.5 https://vulners.com/prion/PRION:CVE-2016-2182
        PRION:CVE-2016-2177 7.5 https://vulners.com/prion/PRION:CVE-2016-2177
        PRION:CVE-2016-1908 7.5 https://vulners.com/prion/PRION:CVE-2016-1908
        PRION:CVE-2015-8668 7.5 https://vulners.com/prion/PRION:CVE-2015-8668
        PRION:CVE-2015-8126 7.5 https://vulners.com/prion/PRION:CVE-2015-8126
        PRION:CVE-2015-4643 7.5 https://vulners.com/prion/PRION:CVE-2015-4643
        PRION:CVE-2015-3329 7.5 https://vulners.com/prion/PRION:CVE-2015-3329
        PRION:CVE-2015-1351 7.5 https://vulners.com/prion/PRION:CVE-2015-1351
        PRION:CVE-2010-5325 7.5 https://vulners.com/prion/PRION:CVE-2010-5325
        MSF:EXPLOIT-UNIX-DHCP-RHEL_DHCP_CLIENT_COMMAND_INJECTION-   7.5 https://vulners.com/metasploit/
MSF:EXPLOIT-UNIX-DHCP-RHEL_DHCP_CLIENT_COMMAND_INJECTION-   *EXPLOIT*
        MSF:AUXILIARY-DOS-DNS-BIND_TSIG-    7.5 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-
BIND_TSIG-  *EXPLOIT*
        EXPLOITPACK:C104DEC6754D1A7A5A100FE10E0C9B31    7.5 https://vulners.com/exploitpack/
```

```
EXPLOITPACK:C104DEC6754D1A7A5A100FE10E0C9B31    *EXPLOIT*
        EDB-ID:44890    7.5 https://vulners.com/exploitdb/EDB-ID:44890  *EXPLOIT*
        EDB-ID:44652    7.5 https://vulners.com/exploitdb/EDB-ID:44652  *EXPLOIT*
        EDB-ID:42091    7.5 https://vulners.com/exploitdb/EDB-ID:42091  *EXPLOIT*
        EDB-ID:40453    7.5 https://vulners.com/exploitdb/EDB-ID:40453  *EXPLOIT*
        CVE-2023-50387  7.5 https://vulners.com/cve/CVE-2023-50387
        CVE-2021-3748   7.5 https://vulners.com/cve/CVE-2021-3748
        CVE-2021-3610   7.5 https://vulners.com/cve/CVE-2021-3610
        CVE-2019-2602   7.5 https://vulners.com/cve/CVE-2019-2602
        CVE-2018-5184   7.5 https://vulners.com/cve/CVE-2018-5184
        CVE-2018-3760   7.5 https://vulners.com/cve/CVE-2018-3760
        CVE-2018-1111   7.5 https://vulners.com/cve/CVE-2018-1111
        CVE-2017-7787   7.5 https://vulners.com/cve/CVE-2017-7787
        CVE-2017-7754   7.5 https://vulners.com/cve/CVE-2017-7754
        CVE-2017-5454   7.5 https://vulners.com/cve/CVE-2017-5454
        CVE-2017-5449   7.5 https://vulners.com/cve/CVE-2017-5449
        CVE-2017-5445   7.5 https://vulners.com/cve/CVE-2017-5445
        CVE-2017-5444   7.5 https://vulners.com/cve/CVE-2017-5444
        CVE-2017-5378   7.5 https://vulners.com/cve/CVE-2017-5378
        CVE-2016-9900   7.5 https://vulners.com/cve/CVE-2016-9900
        CVE-2016-2183   7.5 https://vulners.com/cve/CVE-2016-2183
        CVE-2015-4644   7.5 https://vulners.com/cve/CVE-2015-4644
        CVE-2015-4026   7.5 https://vulners.com/cve/CVE-2015-4026
        CVE-2014-8138   7.5 https://vulners.com/cve/CVE-2014-8138
        CVE-2014-8119   7.5 https://vulners.com/cve/CVE-2014-8119
        CVE-2007-5116   7.5 https://vulners.com/cve/CVE-2007-5116
        CVE-2004-2771   7.5 https://vulners.com/cve/CVE-2004-2771
        BB688FBF-CEE2-5DD1-8561-8F76501DE2D4    7.5 https://vulners.com/githubexploit/BB688FBF-
CEE2-5DD1-8561-8F76501DE2D4 *EXPLOIT*
        1337DAY-ID-32884    7.5 https://vulners.com/zdt/1337DAY-ID-32884    *EXPLOIT*
        CVE-2017-5386   7.3 https://vulners.com/cve/CVE-2017-5386
        SMNTC-110486    7.2 https://vulners.com/symantec/SMNTC-110486
        PRION:CVE-2016-4951 7.2 https://vulners.com/prion/PRION:CVE-2016-4951
        PRION:CVE-2016-4913 7.2 https://vulners.com/prion/PRION:CVE-2016-4913
        PRION:CVE-2016-4805 7.2 https://vulners.com/prion/PRION:CVE-2016-4805
        PRION:CVE-2016-3710 7.2 https://vulners.com/prion/PRION:CVE-2016-3710
        PRION:CVE-2014-1737 7.2 https://vulners.com/prion/PRION:CVE-2014-1737
        PACKETSTORM:148549  7.2 https://vulners.com/packetstorm/PACKETSTORM:148549  *EXPLOIT*
        PACKETSTORM:145391  7.2 https://vulners.com/packetstorm/PACKETSTORM:145391  *EXPLOIT*
        EXPLOITPACK:F4489E070E6CDADA18DE546A030227F0    7.2 https://vulners.com/exploitpack/
EXPLOITPACK:F4489E070E6CDADA18DE546A030227F0    *EXPLOIT*
        EXPLOITPACK:DFB54027B0CAC8B9E041940F5800AB1F    7.2 https://vulners.com/exploitpack/
EXPLOITPACK:DFB54027B0CAC8B9E041940F5800AB1F    *EXPLOIT*
        EXPLOITPACK:D47E67644EBD93EC50A53C69C2A59BBB    7.2 https://vulners.com/exploitpack/
EXPLOITPACK:D47E67644EBD93EC50A53C69C2A59BBB    *EXPLOIT*
        EXPLOITPACK:7C30F59E9F9E9C7EFCD4805D95AF6006    7.2 https://vulners.com/exploitpack/EXPLOITPACK:
7C30F59E9F9E9C7EFCD4805D95AF6006    *EXPLOIT*
        EXPLOITPACK:2E9704BB984395CF6BD1C5E00B34FE96    7.2 https://vulners.com/exploitpack/EXPLOITPACK:
2E9704BB984395CF6BD1C5E00B34FE96    *EXPLOIT*
        EXPLOITPACK:088CF7ADCAFEF383490420614A9EEA47    7.2 https://vulners.com/exploitpack/EXPLOITPACK:
088CF7ADCAFEF383490420614A9EEA47    *EXPLOIT*
        CVE-2015-0412   7.2 https://vulners.com/cve/CVE-2015-0412
        CVE-2013-2231   7.2 https://vulners.com/cve/CVE-2013-2231
        CVE-2013-1813   7.2 https://vulners.com/cve/CVE-2013-1813
        1337DAY-ID-30720    7.2 https://vulners.com/zdt/1337DAY-ID-30720    *EXPLOIT*
        SSV:62080   7.1 https://vulners.com/seebug/SSV:62080    *EXPLOIT*
        PRION:CVE-2014-2706 7.1 https://vulners.com/prion/PRION:CVE-2014-2706
        CVE-2023-1652   7.1 https://vulners.com/cve/CVE-2023-1652
        CVE-2019-10131  7.1 https://vulners.com/cve/CVE-2019-10131
        CVE-2017-1000376    7.0 https://vulners.com/cve/CVE-2017-1000376
        CVE-2014-0143   7.0 https://vulners.com/cve/CVE-2014-0143
        SSV:86729   6.9 https://vulners.com/seebug/SSV:86729    *EXPLOIT*
        SSV:60813   6.9 https://vulners.com/seebug/SSV:60813    *EXPLOIT*
        PRION:CVE-2016-1714 6.9 https://vulners.com/prion/PRION:CVE-2016-1714
```

```
        PRION:CVE-2014-0196 6.9 https://vulners.com/prion/PRION:CVE-2014-0196
        OSV:CVE-2020-11884  6.9 https://vulners.com/osv/OSV:CVE-2020-11884
        EDB-ID:33516    6.9 https://vulners.com/exploitdb/EDB-ID:33516  *EXPLOIT*
        CVE-2013-2224   6.9 https://vulners.com/cve/CVE-2013-2224
        CVE-2013-1976   6.9 https://vulners.com/cve/CVE-2013-1976
        CVE-2011-1011   6.9 https://vulners.com/cve/CVE-2011-1011
        SSV:96477   6.8 https://vulners.com/seebug/SSV:96477    *EXPLOIT*
        PRION:CVE-2018-20346    6.8 https://vulners.com/prion/PRION:CVE-2018-20346
        PRION:CVE-2016-5387 6.8 https://vulners.com/prion/PRION:CVE-2016-5387
        PRION:CVE-2016-5264 6.8 https://vulners.com/prion/PRION:CVE-2016-5264
        PRION:CVE-2016-5263 6.8 https://vulners.com/prion/PRION:CVE-2016-5263
        PRION:CVE-2016-5259 6.8 https://vulners.com/prion/PRION:CVE-2016-5259
        PRION:CVE-2016-5258 6.8 https://vulners.com/prion/PRION:CVE-2016-5258
        PRION:CVE-2016-5252 6.8 https://vulners.com/prion/PRION:CVE-2016-5252
        PRION:CVE-2016-4054 6.8 https://vulners.com/prion/PRION:CVE-2016-4054
        PRION:CVE-2016-4051 6.8 https://vulners.com/prion/PRION:CVE-2016-4051
        PRION:CVE-2016-3606 6.8 https://vulners.com/prion/PRION:CVE-2016-3606
        PRION:CVE-2016-2837 6.8 https://vulners.com/prion/PRION:CVE-2016-2837
        PRION:CVE-2016-2802 6.8 https://vulners.com/prion/PRION:CVE-2016-2802
        PRION:CVE-2016-2801 6.8 https://vulners.com/prion/PRION:CVE-2016-2801
        PRION:CVE-2016-2800 6.8 https://vulners.com/prion/PRION:CVE-2016-2800
        PRION:CVE-2016-2798 6.8 https://vulners.com/prion/PRION:CVE-2016-2798
        PRION:CVE-2016-2797 6.8 https://vulners.com/prion/PRION:CVE-2016-2797
        PRION:CVE-2016-2796 6.8 https://vulners.com/prion/PRION:CVE-2016-2796
        PRION:CVE-2016-2795 6.8 https://vulners.com/prion/PRION:CVE-2016-2795
        PRION:CVE-2016-2793 6.8 https://vulners.com/prion/PRION:CVE-2016-2793
        PRION:CVE-2016-2792 6.8 https://vulners.com/prion/PRION:CVE-2016-2792
        PRION:CVE-2016-2791 6.8 https://vulners.com/prion/PRION:CVE-2016-2791
        PRION:CVE-2016-2790 6.8 https://vulners.com/prion/PRION:CVE-2016-2790
        PRION:CVE-2016-1977 6.8 https://vulners.com/prion/PRION:CVE-2016-1977
        PRION:CVE-2016-1974 6.8 https://vulners.com/prion/PRION:CVE-2016-1974
        PRION:CVE-2016-1973 6.8 https://vulners.com/prion/PRION:CVE-2016-1973
        PRION:CVE-2016-1966 6.8 https://vulners.com/prion/PRION:CVE-2016-1966
        PRION:CVE-2016-1964 6.8 https://vulners.com/prion/PRION:CVE-2016-1964
        PRION:CVE-2016-1961 6.8 https://vulners.com/prion/PRION:CVE-2016-1961
        PRION:CVE-2016-1960 6.8 https://vulners.com/prion/PRION:CVE-2016-1960
        PRION:CVE-2016-1954 6.8 https://vulners.com/prion/PRION:CVE-2016-1954
        PRION:CVE-2016-1952 6.8 https://vulners.com/prion/PRION:CVE-2016-1952
        PRION:CVE-2016-1950 6.8 https://vulners.com/prion/PRION:CVE-2016-1950
        PRION:CVE-2015-7512 6.8 https://vulners.com/prion/PRION:CVE-2015-7512
        PRION:CVE-2015-3330 6.8 https://vulners.com/prion/PRION:CVE-2015-3330
        PACKETSTORM:146819  6.8 https://vulners.com/packetstorm/PACKETSTORM:146819  *EXPLOIT*
        PACKETSTORM:143867  6.8 https://vulners.com/packetstorm/PACKETSTORM:143867  *EXPLOIT*
        CVE-2015-3330   6.8 https://vulners.com/cve/CVE-2015-3330
        CVE-2013-4397   6.8 https://vulners.com/cve/CVE-2013-4397
        CVE-2012-3406   6.8 https://vulners.com/cve/CVE-2012-3406
        CVE-2011-4111   6.8 https://vulners.com/cve/CVE-2011-4111
        1337DAY-ID-28309    6.8 https://vulners.com/zdt/1337DAY-ID-28309    *EXPLOIT*
        CVE-2023-2194   6.7 https://vulners.com/cve/CVE-2023-2194
        CVE-2022-40982  6.5 https://vulners.com/cve/CVE-2022-40982
        CVE-2022-2850   6.5 https://vulners.com/cve/CVE-2022-2850
        CVE-2021-4145   6.5 https://vulners.com/cve/CVE-2021-4145
        CVE-2021-3930   6.5 https://vulners.com/cve/CVE-2021-3930
        CVE-2021-3596   6.5 https://vulners.com/cve/CVE-2021-3596
        CVE-2018-12373  6.5 https://vulners.com/cve/CVE-2018-12373
        CVE-2018-12372  6.5 https://vulners.com/cve/CVE-2018-12372
        CVE-2018-10872  6.5 https://vulners.com/cve/CVE-2018-10872
        CVE-2017-5407   6.5 https://vulners.com/cve/CVE-2017-5407
        CVE-2015-3411   6.5 https://vulners.com/cve/CVE-2015-3411
        CAF53201-1371-591C-BFC7-4BA2A958F08A    6.5 https://vulners.com/githubexploit/CAF53201-1371-591C-
BFC7-4BA2A958F08A   *EXPLOIT*
        294A2C02-1F46-5A48-915D-92DDD89915A1    6.5 https://vulners.com/githubexploit/
294A2C02-1F46-5A48-915D-92DDD89915A1    *EXPLOIT*
        PRION:CVE-2014-8566 6.4 https://vulners.com/prion/PRION:CVE-2014-8566
```

```
        CVE-2013-2561   6.3 https://vulners.com/cve/CVE-2013-2561
        CVE-2013-4482   6.2 https://vulners.com/cve/CVE-2013-4482
        CVE-2012-5536   6.2 https://vulners.com/cve/CVE-2012-5536
        CVE-2021-3507   6.1 https://vulners.com/cve/CVE-2021-3507
        CVE-2021-20208  6.1 https://vulners.com/cve/CVE-2021-20208
        CVE-2017-5466   6.1 https://vulners.com/cve/CVE-2017-5466
        CVE-2016-9895   6.1 https://vulners.com/cve/CVE-2016-9895
        CVE-2019-2684   5.9 https://vulners.com/cve/CVE-2019-2684
        CVE-2018-18506  5.9 https://vulners.com/cve/CVE-2018-18506
        CVE-2022-2393   5.7 https://vulners.com/cve/CVE-2022-2393
        CVE-2013-1935   5.7 https://vulners.com/cve/CVE-2013-1935
        CVE-2011-3593   5.7 https://vulners.com/cve/CVE-2011-3593
        CVE-2011-0714   5.7 https://vulners.com/cve/CVE-2011-0714
        CVE-2005-0109   5.6 https://vulners.com/cve/CVE-2005-0109
        SSV:61967   5.5 https://vulners.com/seebug/SSV:61967    *EXPLOIT*
        CVE-2023-3161   5.5 https://vulners.com/cve/CVE-2023-3161
        CVE-2023-28328  5.5 https://vulners.com/cve/CVE-2023-28328
        CVE-2023-1095   5.5 https://vulners.com/cve/CVE-2023-1095
        CVE-2022-3707   5.5 https://vulners.com/cve/CVE-2022-3707
        CVE-2022-2905   5.5 https://vulners.com/cve/CVE-2022-2905
        CVE-2022-0530   5.5 https://vulners.com/cve/CVE-2022-0530
        CVE-2022-0529   5.5 https://vulners.com/cve/CVE-2022-0529
        CVE-2021-20246  5.5 https://vulners.com/cve/CVE-2021-20246
        CVE-2021-20245  5.5 https://vulners.com/cve/CVE-2021-20245
        CVE-2021-20244  5.5 https://vulners.com/cve/CVE-2021-20244
        CVE-2017-15121  5.5 https://vulners.com/cve/CVE-2017-15121
        CVE-2016-0666   5.5 https://vulners.com/cve/CVE-2016-0666
        CVE-2016-0665   5.5 https://vulners.com/cve/CVE-2016-0665
        CVE-2014-0055   5.5 https://vulners.com/cve/CVE-2014-0055
        CVE-2015-0383   5.4 https://vulners.com/cve/CVE-2015-0383
        CVE-2019-2769   5.3 https://vulners.com/cve/CVE-2019-2769
        CVE-2019-2762   5.3 https://vulners.com/cve/CVE-2019-2762
        CVE-2018-5117   5.3 https://vulners.com/cve/CVE-2018-5117
        CVE-2017-7848   5.3 https://vulners.com/cve/CVE-2017-7848
        CVE-2017-7791   5.3 https://vulners.com/cve/CVE-2017-7791
        CVE-2017-5408   5.3 https://vulners.com/cve/CVE-2017-5408
        CVE-2017-5405   5.3 https://vulners.com/cve/CVE-2017-5405
        CVE-2017-5383   5.3 https://vulners.com/cve/CVE-2017-5383
        PRION:CVE-2016-5388 5.1 https://vulners.com/prion/PRION:CVE-2016-5388
        PRION:CVE-2016-5385 5.1 https://vulners.com/prion/PRION:CVE-2016-5385
        CVE-2022-3500   5.1 https://vulners.com/cve/CVE-2022-3500
        SSV:62058   5.0 https://vulners.com/seebug/SSV:62058    *EXPLOIT*
        SSV:60818   5.0 https://vulners.com/seebug/SSV:60818    *EXPLOIT*
        SSV:60814   5.0 https://vulners.com/seebug/SSV:60814    *EXPLOIT*
        SSV:60051   5.0 https://vulners.com/seebug/SSV:60051    *EXPLOIT*
        SMNTC-110517    5.0 https://vulners.com/symantec/SMNTC-110517
        PRION:CVE-2018-17962    5.0 https://vulners.com/prion/PRION:CVE-2018-17962
        PRION:CVE-2016-6302 5.0 https://vulners.com/prion/PRION:CVE-2016-6302
        PRION:CVE-2016-5418 5.0 https://vulners.com/prion/PRION:CVE-2016-5418
        PRION:CVE-2016-4809 5.0 https://vulners.com/prion/PRION:CVE-2016-4809
        PRION:CVE-2016-4556 5.0 https://vulners.com/prion/PRION:CVE-2016-4556
        PRION:CVE-2016-4555 5.0 https://vulners.com/prion/PRION:CVE-2016-4555
        PRION:CVE-2016-4554 5.0 https://vulners.com/prion/PRION:CVE-2016-4554
        PRION:CVE-2016-3508 5.0 https://vulners.com/prion/PRION:CVE-2016-3508
        PRION:CVE-2016-3500 5.0 https://vulners.com/prion/PRION:CVE-2016-3500
        PRION:CVE-2016-2518 5.0 https://vulners.com/prion/PRION:CVE-2016-2518
        PRION:CVE-2016-2181 5.0 https://vulners.com/prion/PRION:CVE-2016-2181
        PRION:CVE-2016-2180 5.0 https://vulners.com/prion/PRION:CVE-2016-2180
        PRION:CVE-2016-2179 5.0 https://vulners.com/prion/PRION:CVE-2016-2179
        PRION:CVE-2015-8000 5.0 https://vulners.com/prion/PRION:CVE-2015-8000
        PRION:CVE-2015-7701 5.0 https://vulners.com/prion/PRION:CVE-2015-7701
        PRION:CVE-2015-7692 5.0 https://vulners.com/prion/PRION:CVE-2015-7692
        PRION:CVE-2015-7691 5.0 https://vulners.com/prion/PRION:CVE-2015-7691
        PRION:CVE-2015-5219 5.0 https://vulners.com/prion/PRION:CVE-2015-5219
```

```
        PRION:CVE-2015-4024 5.0 https://vulners.com/prion/PRION:CVE-2015-4024
        PRION:CVE-2015-3195 5.0 https://vulners.com/prion/PRION:CVE-2015-3195
        PRION:CVE-2014-3581 5.0 https://vulners.com/prion/PRION:CVE-2014-3581
        PRION:CVE-2013-5704 5.0 https://vulners.com/prion/PRION:CVE-2013-5704
        PRION:CVE-2013-5211 5.0 https://vulners.com/prion/PRION:CVE-2013-5211
        PACKETSTORM:142756  5.0 https://vulners.com/packetstorm/PACKETSTORM:142756  *EXPLOIT*
        OSV:CVE-2019-18282  5.0 https://vulners.com/osv/OSV:CVE-2019-18282
        OSV:CVE-2018-1751   5.0 https://vulners.com/osv/OSV:CVE-2018-1751
        MSF:AUXILIARY-SCANNER-NTP-NTP_MONLIST-  5.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-
NTP-NTP_MONLIST-    *EXPLOIT*
        EDB-ID:33073    5.0 https://vulners.com/exploitdb/EDB-ID:33073  *EXPLOIT*
        CVE-2015-4024   5.0 https://vulners.com/cve/CVE-2015-4024
        CVE-2015-0407   5.0 https://vulners.com/cve/CVE-2015-0407
        CVE-2014-3562   5.0 https://vulners.com/cve/CVE-2014-3562
        CVE-2012-3405   5.0 https://vulners.com/cve/CVE-2012-3405
        CVE-2012-3404   5.0 https://vulners.com/cve/CVE-2012-3404
        SSV:62220   4.9 https://vulners.com/seebug/SSV:62220    *EXPLOIT*
        PRION:CVE-2016-6198 4.9 https://vulners.com/prion/PRION:CVE-2016-6198
        PRION:CVE-2016-6197 4.9 https://vulners.com/prion/PRION:CVE-2016-6197
        PRION:CVE-2016-5403 4.9 https://vulners.com/prion/PRION:CVE-2016-5403
        PRION:CVE-2016-4581 4.9 https://vulners.com/prion/PRION:CVE-2016-4581
        PRION:CVE-2016-4470 4.9 https://vulners.com/prion/PRION:CVE-2016-4470
        PRION:CVE-2014-3145 4.9 https://vulners.com/prion/PRION:CVE-2014-3145
        PRION:CVE-2014-3144 4.9 https://vulners.com/prion/PRION:CVE-2014-3144
        PRION:CVE-2014-0203 4.9 https://vulners.com/prion/PRION:CVE-2014-0203
        PRION:CVE-2013-4312 4.9 https://vulners.com/prion/PRION:CVE-2013-4312
        CVE-2014-0150   4.9 https://vulners.com/cve/CVE-2014-0150
        CVE-2020-2655   4.8 https://vulners.com/cve/CVE-2020-2655
        CVE-2019-2816   4.8 https://vulners.com/cve/CVE-2019-2816
        SPECTRE_SAM_LEAK    4.7 https://vulners.com/canvas/SPECTRE_SAM_LEAK *EXPLOIT*
        SPECTRE_FILE_LEAK   4.7 https://vulners.com/canvas/SPECTRE_FILE_LEAK    *EXPLOIT*
        SMNTC-102378    4.7 https://vulners.com/symantec/SMNTC-102378
        SMNTC-102371    4.7 https://vulners.com/symantec/SMNTC-102371
        OSV:CVE-2019-15902  4.7 https://vulners.com/osv/OSV:CVE-2019-15902
        CVE-2013-2188   4.7 https://vulners.com/cve/CVE-2013-2188
        1337DAY-ID-29366    4.7 https://vulners.com/zdt/1337DAY-ID-29366    *EXPLOIT*
        PRION:CVE-2022-21499    4.6 https://vulners.com/prion/PRION:CVE-2022-21499
        PRION:CVE-2016-0617 4.6 https://vulners.com/prion/PRION:CVE-2016-0617
        CVE-2011-3347   4.6 https://vulners.com/cve/CVE-2011-3347
        CVE-2023-2019   4.4 https://vulners.com/cve/CVE-2023-2019
        SSV:61028   4.3 https://vulners.com/seebug/SSV:61028    *EXPLOIT*
        SMNTC-107260    4.3 https://vulners.com/symantec/SMNTC-107260
        PRION:CVE-2016-7166 4.3 https://vulners.com/prion/PRION:CVE-2016-7166
        PRION:CVE-2016-5844 4.3 https://vulners.com/prion/PRION:CVE-2016-5844
        PRION:CVE-2016-5262 4.3 https://vulners.com/prion/PRION:CVE-2016-5262
        PRION:CVE-2016-4053 4.3 https://vulners.com/prion/PRION:CVE-2016-4053
        PRION:CVE-2016-3550 4.3 https://vulners.com/prion/PRION:CVE-2016-3550
        PRION:CVE-2016-3458 4.3 https://vulners.com/prion/PRION:CVE-2016-3458
        PRION:CVE-2016-1965 4.3 https://vulners.com/prion/PRION:CVE-2016-1965
        PRION:CVE-2016-1958 4.3 https://vulners.com/prion/PRION:CVE-2016-1958
        PRION:CVE-2016-1957 4.3 https://vulners.com/prion/PRION:CVE-2016-1957
        PRION:CVE-2015-8896 4.3 https://vulners.com/prion/PRION:CVE-2015-8896
        PRION:CVE-2015-7977 4.3 https://vulners.com/prion/PRION:CVE-2015-7977
        PRION:CVE-2015-7852 4.3 https://vulners.com/prion/PRION:CVE-2015-7852
        PRION:CVE-2015-7703 4.3 https://vulners.com/prion/PRION:CVE-2015-7703
        OSV:CVE-2023-5972   4.3 https://vulners.com/osv/OSV:CVE-2023-5972
        OSV:CVE-2023-51042  4.3 https://vulners.com/osv/OSV:CVE-2023-51042
        OSV:CVE-2023-45898  4.3 https://vulners.com/osv/OSV:CVE-2023-45898
        OSV:CVE-2020-13143  4.3 https://vulners.com/osv/OSV:CVE-2020-13143
        CVE-2023-6121   4.3 https://vulners.com/cve/CVE-2023-6121
        CVE-2018-12374  4.3 https://vulners.com/cve/CVE-2018-12374
        CVE-2017-5451   4.3 https://vulners.com/cve/CVE-2017-5451
        CVE-2013-4287   4.3 https://vulners.com/cve/CVE-2013-4287
        CVE-2013-1857   4.3 https://vulners.com/cve/CVE-2013-1857
```

chowkidar

```
CVE-2013-1824   4.3 https://vulners.com/cve/CVE-2013-1824
CVE-2013-0281   4.3 https://vulners.com/cve/CVE-2013-0281
CVE-2013-0221   4.3 https://vulners.com/cve/CVE-2013-0221
CVE-2012-4546   4.3 https://vulners.com/cve/CVE-2012-4546
SMNTC-106843    4.0 https://vulners.com/symantec/SMNTC-106843
PRION:CVE-2016-5404 4.0 https://vulners.com/prion/PRION:CVE-2016-5404
PRION:CVE-2016-5265 4.0 https://vulners.com/prion/PRION:CVE-2016-5265
PRION:CVE-2015-8631 4.0 https://vulners.com/prion/PRION:CVE-2015-8631
PRION:CVE-2015-7702 4.0 https://vulners.com/prion/PRION:CVE-2015-7702
OSV:CVE-2023-3338   4.0 https://vulners.com/osv/OSV:CVE-2023-3338
CVE-2016-0597   4.0 https://vulners.com/cve/CVE-2016-0597
CVE-2016-0595   4.0 https://vulners.com/cve/CVE-2016-0595
CVE-2015-4800   4.0 https://vulners.com/cve/CVE-2015-4800
CVE-2015-4756   4.0 https://vulners.com/cve/CVE-2015-4756
CVE-2014-3940   4.0 https://vulners.com/cve/CVE-2014-3940
CVE-2013-4485   4.0 https://vulners.com/cve/CVE-2013-4485
CVE-2016-3452   3.7 https://vulners.com/cve/CVE-2016-3452
CVE-2012-0787   3.7 https://vulners.com/cve/CVE-2012-0787
OSV:CVE-2023-6546   3.5 https://vulners.com/osv/OSV:CVE-2023-6546
OSV:CVE-2023-51782  3.5 https://vulners.com/osv/OSV:CVE-2023-51782
OSV:CVE-2023-51781  3.5 https://vulners.com/osv/OSV:CVE-2023-51781
OSV:CVE-2023-51780  3.5 https://vulners.com/osv/OSV:CVE-2023-51780
OSV:CVE-2023-51043  3.5 https://vulners.com/osv/OSV:CVE-2023-51043
OSV:CVE-2023-2006   3.5 https://vulners.com/osv/OSV:CVE-2023-2006
CVE-2016-0600   3.5 https://vulners.com/cve/CVE-2016-0600
CVE-2015-4890   3.5 https://vulners.com/cve/CVE-2015-4890
CVE-2019-2786   3.4 https://vulners.com/cve/CVE-2019-2786
CVE-2021-4217   3.3 https://vulners.com/cve/CVE-2021-4217
CVE-2020-27776  3.3 https://vulners.com/cve/CVE-2020-27776
CVE-2020-27775  3.3 https://vulners.com/cve/CVE-2020-27775
CVE-2020-27774  3.3 https://vulners.com/cve/CVE-2020-27774
CVE-2020-27773  3.3 https://vulners.com/cve/CVE-2020-27773
CVE-2020-27772  3.3 https://vulners.com/cve/CVE-2020-27772
CVE-2020-27771  3.3 https://vulners.com/cve/CVE-2020-27771
CVE-2020-27767  3.3 https://vulners.com/cve/CVE-2020-27767
CVE-2020-27765  3.3 https://vulners.com/cve/CVE-2020-27765
CVE-2014-0249   3.3 https://vulners.com/cve/CVE-2014-0249
CVE-2020-14394  3.2 https://vulners.com/cve/CVE-2020-14394
CVE-2016-0607   2.8 https://vulners.com/cve/CVE-2016-0607
PRION:CVE-2016-0695 2.6 https://vulners.com/prion/PRION:CVE-2016-0695
CVE-2013-2051   2.6 https://vulners.com/cve/CVE-2013-2051
CVE-2021-3923   2.3 https://vulners.com/cve/CVE-2021-3923
PRION:CVE-2016-2178 2.1 https://vulners.com/prion/PRION:CVE-2016-2178
PRION:CVE-2015-8629 2.1 https://vulners.com/prion/PRION:CVE-2015-8629
PRION:CVE-2014-9644 2.1 https://vulners.com/prion/PRION:CVE-2014-9644
PRION:CVE-2014-1738 2.1 https://vulners.com/prion/PRION:CVE-2014-1738
PRION:CVE-2013-7421 2.1 https://vulners.com/prion/PRION:CVE-2013-7421
OSV:CVE-2021-28039  2.1 https://vulners.com/osv/OSV:CVE-2021-28039
OSV:CVE-2020-9391   2.1 https://vulners.com/osv/OSV:CVE-2020-9391
CVE-2016-0605   2.1 https://vulners.com/cve/CVE-2016-0605
CVE-2013-2164   2.1 https://vulners.com/cve/CVE-2013-2164
CVE-2013-0222   2.1 https://vulners.com/cve/CVE-2013-0222
SSV:60002   1.9 https://vulners.com/seebug/SSV:60002    *EXPLOIT*
PRION:CVE-2014-8134 1.9 https://vulners.com/prion/PRION:CVE-2014-8134
OSV:CVE-2021-26932  1.9 https://vulners.com/osv/OSV:CVE-2021-26932
CVE-2013-4481   1.9 https://vulners.com/cve/CVE-2013-4481
CVE-2013-0223   1.9 https://vulners.com/cve/CVE-2013-0223
CVE-2012-6545   1.9 https://vulners.com/cve/CVE-2012-6545
CVE-2012-1568   1.9 https://vulners.com/cve/CVE-2012-1568
CVE-2011-2693   1.9 https://vulners.com/cve/CVE-2011-2693
PRION:CVE-2023-22024    1.7 https://vulners.com/prion/PRION:CVE-2023-22024
OSV:CVE-2023-6915   1.7 https://vulners.com/osv/OSV:CVE-2023-6915
OSV:CVE-2023-6039   1.7 https://vulners.com/osv/OSV:CVE-2023-6039
CVE-2014-5177   1.2 https://vulners.com/cve/CVE-2014-5177
```

```
        OSV:CVE-2023-46862  1.0 https://vulners.com/osv/OSV:CVE-2023-46862
        SSV:97466   0.0 https://vulners.com/seebug/SSV:97466    *EXPLOIT*
        SSV:97290   0.0 https://vulners.com/seebug/SSV:97290    *EXPLOIT*
        SSV:97059   0.0 https://vulners.com/seebug/SSV:97059    *EXPLOIT*
        SSV:93154   0.0 https://vulners.com/seebug/SSV:93154    *EXPLOIT*
        SSV:93152   0.0 https://vulners.com/seebug/SSV:93152    *EXPLOIT*
        SSV:92853   0.0 https://vulners.com/seebug/SSV:92853    *EXPLOIT*
        SSV:92622   0.0 https://vulners.com/seebug/SSV:92622    *EXPLOIT*
        SMNTC-111446    0.0 https://vulners.com/symantec/SMNTC-111446
        SMNTC-111409    0.0 https://vulners.com/symantec/SMNTC-111409
        SMNTC-111365    0.0 https://vulners.com/symantec/SMNTC-111365
        SMNTC-111183    0.0 https://vulners.com/symantec/SMNTC-111183
        SMNTC-110978    0.0 https://vulners.com/symantec/SMNTC-110978
        SMNTC-110846    0.0 https://vulners.com/symantec/SMNTC-110846
        SMNTC-110842    0.0 https://vulners.com/symantec/SMNTC-110842
        SMNTC-110841    0.0 https://vulners.com/symantec/SMNTC-110841
        SMNTC-110579    0.0 https://vulners.com/symantec/SMNTC-110579
        SMNTC-110577    0.0 https://vulners.com/symantec/SMNTC-110577
        SMNTC-110422    0.0 https://vulners.com/symantec/SMNTC-110422
        SMNTC-107485    0.0 https://vulners.com/symantec/SMNTC-107485
        SMNTC-106116    0.0 https://vulners.com/symantec/SMNTC-106116
        SMNTC-103708    0.0 https://vulners.com/symantec/SMNTC-103708
        PACKETSTORM:148172  0.0 https://vulners.com/packetstorm/PACKETSTORM:148172  *EXPLOIT*
        PACKETSTORM:147698  0.0 https://vulners.com/packetstorm/PACKETSTORM:147698  *EXPLOIT*
        PACKETSTORM:145645  0.0 https://vulners.com/packetstorm/PACKETSTORM:145645  *EXPLOIT*
        PACKETSTORM:142670  0.0 https://vulners.com/packetstorm/PACKETSTORM:142670  *EXPLOIT*
        PACKETSTORM:142668  0.0 https://vulners.com/packetstorm/PACKETSTORM:142668  *EXPLOIT*
        PACKETSTORM:140491  0.0 https://vulners.com/packetstorm/PACKETSTORM:140491  *EXPLOIT*
        OSV:CVE-2023-51779  0.0 https://vulners.com/osv/OSV:CVE-2023-51779
        1337DAY-ID-31839    0.0 https://vulners.com/zdt/1337DAY-ID-31839    *EXPLOIT*
        1337DAY-ID-30727    0.0 https://vulners.com/zdt/1337DAY-ID-30727    *EXPLOIT*
        1337DAY-ID-30581    0.0 https://vulners.com/zdt/1337DAY-ID-30581    *EXPLOIT*
        1337DAY-ID-30427    0.0 https://vulners.com/zdt/1337DAY-ID-30427    *EXPLOIT*
        1337DAY-ID-30372    0.0 https://vulners.com/zdt/1337DAY-ID-30372    *EXPLOIT*
        1337DAY-ID-30247    0.0 https://vulners.com/zdt/1337DAY-ID-30247    *EXPLOIT*
        1337DAY-ID-30246    0.0 https://vulners.com/zdt/1337DAY-ID-30246    *EXPLOIT*
        1337DAY-ID-30245    0.0 https://vulners.com/zdt/1337DAY-ID-30245    *EXPLOIT*
        1337DAY-ID-30244    0.0 https://vulners.com/zdt/1337DAY-ID-30244    *EXPLOIT*
        1337DAY-ID-27840    0.0 https://vulners.com/zdt/1337DAY-ID-27840    *EXPLOIT*
        1337DAY-ID-27839    0.0 https://vulners.com/zdt/1337DAY-ID-27839    *EXPLOIT*
        1337DAY-ID-27356    0.0 https://vulners.com/zdt/1337DAY-ID-27356    *EXPLOIT*
        1337DAY-ID-26670    0.0 https://vulners.com/zdt/1337DAY-ID-26670    *EXPLOIT*


465 smtp 4.87
  cpe:/a:exim:exim:4.87:
        SMNTC-110023    10.0    https://vulners.com/symantec/SMNTC-110023
        PRION:CVE-2019-15846    10.0    https://vulners.com/prion/PRION:CVE-2019-15846
        PRION:CVE-2019-13917    10.0    https://vulners.com/prion/PRION:CVE-2019-13917
        PRION:CVE-2019-10149    10.0    https://vulners.com/prion/PRION:CVE-2019-10149
        F89047E2-C89C-5590-9779-EAEEE60078B9    10.0    https://vulners.com/githubexploit/F89047E2-
C89C-5590-9779-EAEEE60078B9 *EXPLOIT*
        EXPLOITPACK:4FFD4258EB9240F56C83A57C965E0913    10.0    https://vulners.com/exploitpack/
EXPLOITPACK:4FFD4258EB9240F56C83A57C965E0913    *EXPLOIT*
        EXIM_EXPANSION_RCE  10.0    https://vulners.com/canvas/EXIM_EXPANSION_RCE   *EXPLOIT*
        E1FEC345-BB7E-5FFE-AD78-64A1B9E93172    10.0    https://vulners.com/githubexploit/E1FEC345-
BB7E-5FFE-AD78-64A1B9E93172 *EXPLOIT*
        ADA0DDA5-BF6D-5656-87DA-B9E2BF0777ED    10.0    https://vulners.com/githubexploit/ADA0DDA5-
BF6D-5656-87DA-B9E2BF0777ED *EXPLOIT*
        910B7127-C06A-533E-BFC7-6ED36944EA87    10.0    https://vulners.com/githubexploit/910B7127-
C06A-533E-BFC7-6ED36944EA87 *EXPLOIT*
        7DB4D6C1-099F-581F-8C39-DB454925C570    10.0    https://vulners.com/githubexploit/
7DB4D6C1-099F-581F-8C39-DB454925C570    *EXPLOIT*
        7B7215E0-65A8-5ECC-B222-5204D0DE0ABF    10.0    https://vulners.com/githubexploit/
```

```
7B7215E0-65A8-5ECC-B222-5204D0DE0ABF    *EXPLOIT*
        53BB099A-E497-5170-9B4B-16FB5A78CF67    10.0    https://vulners.com/githubexploit/53BB099A-
E497-5170-9B4B-16FB5A78CF67 *EXPLOIT*
        314FBFEA-2B26-54C6-BD8B-833438155879    10.0    https://vulners.com/githubexploit/
314FBFEA-2B26-54C6-BD8B-833438155879    *EXPLOIT*
        1337DAY-ID-32848    10.0    https://vulners.com/zdt/1337DAY-ID-32848    *EXPLOIT*
        SAINT:A9B0B05DC77287BBA5CCE7B14B30EB70  9.8 https://vulners.com/saint/
SAINT:A9B0B05DC77287BBA5CCE7B14B30EB70  *EXPLOIT*
        SAINT:7C1EF5B76FC3A237B68C699EF952633A  9.8 https://vulners.com/saint/SAINT:
7C1EF5B76FC3A237B68C699EF952633A    *EXPLOIT*
        MSF:EXPLOIT-LINUX-LOCAL-EXIM4_DELIVER_MESSAGE_PRIV_ESC- 9.8 https://vulners.com/metasploit/
MSF:EXPLOIT-LINUX-LOCAL-EXIM4_DELIVER_MESSAGE_PRIV_ESC- *EXPLOIT*
        EDB-ID:47307    9.8 https://vulners.com/exploitdb/EDB-ID:47307  *EXPLOIT*
        EDB-ID:46996    9.8 https://vulners.com/exploitdb/EDB-ID:46996  *EXPLOIT*
        EDB-ID:46974    9.8 https://vulners.com/exploitdb/EDB-ID:46974  *EXPLOIT*
        EDB-ID:45671    9.8 https://vulners.com/exploitdb/EDB-ID:45671  *EXPLOIT*
        EDB-ID:44571    9.8 https://vulners.com/exploitdb/EDB-ID:44571  *EXPLOIT*
        CVE-2022-37452  9.8 https://vulners.com/cve/CVE-2022-37452
        CVE-2020-28026  9.8 https://vulners.com/cve/CVE-2020-28026
        CVE-2020-28024  9.8 https://vulners.com/cve/CVE-2020-28024
        CVE-2020-28022  9.8 https://vulners.com/cve/CVE-2020-28022
        CVE-2020-28020  9.8 https://vulners.com/cve/CVE-2020-28020
        CVE-2020-28017  9.8 https://vulners.com/cve/CVE-2020-28017
        CVE-2019-15846  9.8 https://vulners.com/cve/CVE-2019-15846
        CVE-2019-13917  9.8 https://vulners.com/cve/CVE-2019-13917
        CVE-2019-10149  9.8 https://vulners.com/cve/CVE-2019-10149
        CVE-2018-6789   9.8 https://vulners.com/cve/CVE-2018-6789
        1337DAY-ID-36350    9.8 https://vulners.com/zdt/1337DAY-ID-36350    *EXPLOIT*
        PRION:CVE-2020-28026    9.3 https://vulners.com/prion/PRION:CVE-2020-28026
        PRION:CVE-2020-28021    9.0 https://vulners.com/prion/PRION:CVE-2020-28021
        CVE-2020-28021  8.8 https://vulners.com/cve/CVE-2020-28021
        CVE-2020-28016  7.8 https://vulners.com/cve/CVE-2020-28016
        CVE-2020-28015  7.8 https://vulners.com/cve/CVE-2020-28015
        CVE-2020-28013  7.8 https://vulners.com/cve/CVE-2020-28013
        CVE-2020-28012  7.8 https://vulners.com/cve/CVE-2020-28012
        CVE-2020-28011  7.8 https://vulners.com/cve/CVE-2020-28011
        CVE-2020-28010  7.8 https://vulners.com/cve/CVE-2020-28010
        CVE-2020-28009  7.8 https://vulners.com/cve/CVE-2020-28009
        CVE-2020-28008  7.8 https://vulners.com/cve/CVE-2020-28008
        CVE-2020-28007  7.8 https://vulners.com/cve/CVE-2020-28007
        SSV:99253   7.5 https://vulners.com/seebug/SSV:99253    *EXPLOIT*
        SSV:97269   7.5 https://vulners.com/seebug/SSV:97269    *EXPLOIT*
        SAINT:4A51F090FB88D7C0687C235D80825104  7.5 https://vulners.com/saint/SAINT:
4A51F090FB88D7C0687C235D80825104    *EXPLOIT*
        PRION:CVE-2022-37452    7.5 https://vulners.com/prion/PRION:CVE-2022-37452
        PRION:CVE-2020-28024    7.5 https://vulners.com/prion/PRION:CVE-2020-28024
        PRION:CVE-2020-28022    7.5 https://vulners.com/prion/PRION:CVE-2020-28022
        PRION:CVE-2020-28020    7.5 https://vulners.com/prion/PRION:CVE-2020-28020
        PRION:CVE-2020-28018    7.5 https://vulners.com/prion/PRION:CVE-2020-28018
        PRION:CVE-2020-28017    7.5 https://vulners.com/prion/PRION:CVE-2020-28017
        PRION:CVE-2019-16928    7.5 https://vulners.com/prion/PRION:CVE-2019-16928
        PRION:CVE-2018-6789 7.5 https://vulners.com/prion/PRION:CVE-2018-6789
        PACKETSTORM:162959  7.5 https://vulners.com/packetstorm/PACKETSTORM:162959  *EXPLOIT*
        PACKETSTORM:154198  7.5 https://vulners.com/packetstorm/PACKETSTORM:154198  *EXPLOIT*
        PACKETSTORM:153312  7.5 https://vulners.com/packetstorm/PACKETSTORM:153312  *EXPLOIT*
        PACKETSTORM:149926  7.5 https://vulners.com/packetstorm/PACKETSTORM:149926  *EXPLOIT*
        PACKETSTORM:147456  7.5 https://vulners.com/packetstorm/PACKETSTORM:147456  *EXPLOIT*
        EXPLOITPACK:D1236C309752040951CA6CF70D1EEE69    7.5 https://vulners.com/exploitpack/
EXPLOITPACK:D1236C309752040951CA6CF70D1EEE69    *EXPLOIT*
        EXPLOITPACK:5F07E65256D3B05FE6074E80F7346498    7.5 https://vulners.com/exploitpack/EXPLOITPACK:
5F07E65256D3B05FE6074E80F7346498    *EXPLOIT*
        EXPLOITPACK:4639A09DD9AC0CEB700BE689515D2AE7    7.5 https://vulners.com/exploitpack/EXPLOITPACK:
4639A09DD9AC0CEB700BE689515D2AE7    *EXPLOIT*
        EXIM_HEAP_OVERFLOW  7.5 https://vulners.com/canvas/EXIM_HEAP_OVERFLOW   *EXPLOIT*
```

```
        CVE-2022-37451  7.5 https://vulners.com/cve/CVE-2022-37451
        CVE-2021-38371  7.5 https://vulners.com/cve/CVE-2021-38371
        CVE-2020-28025  7.5 https://vulners.com/cve/CVE-2020-28025
        CVE-2020-28023  7.5 https://vulners.com/cve/CVE-2020-28023
        CVE-2020-12783  7.5 https://vulners.com/cve/CVE-2020-12783
        CHAINGUARD:CVE-2023-42115   7.5 https://vulners.com/cgr/CHAINGUARD:CVE-2023-42115
        1337DAY-ID-33150    7.5 https://vulners.com/zdt/1337DAY-ID-33150    *EXPLOIT*
        1337DAY-ID-32869    7.5 https://vulners.com/zdt/1337DAY-ID-32869    *EXPLOIT*
        1337DAY-ID-31403    7.5 https://vulners.com/zdt/1337DAY-ID-31403    *EXPLOIT*
        1337DAY-ID-30290    7.5 https://vulners.com/zdt/1337DAY-ID-30290    *EXPLOIT*
        PRION:CVE-2020-28016    7.2 https://vulners.com/prion/PRION:CVE-2020-28016
        PRION:CVE-2020-28015    7.2 https://vulners.com/prion/PRION:CVE-2020-28015
        PRION:CVE-2020-28013    7.2 https://vulners.com/prion/PRION:CVE-2020-28013
        PRION:CVE-2020-28012    7.2 https://vulners.com/prion/PRION:CVE-2020-28012
        PRION:CVE-2020-28011    7.2 https://vulners.com/prion/PRION:CVE-2020-28011
        PRION:CVE-2020-28010    7.2 https://vulners.com/prion/PRION:CVE-2020-28010
        PRION:CVE-2020-28009    7.2 https://vulners.com/prion/PRION:CVE-2020-28009
        PRION:CVE-2020-28008    7.2 https://vulners.com/prion/PRION:CVE-2020-28008
        PRION:CVE-2020-28007    7.2 https://vulners.com/prion/PRION:CVE-2020-28007
        PRION:CVE-2021-27216    6.3 https://vulners.com/prion/PRION:CVE-2021-27216
        CVE-2021-27216  6.3 https://vulners.com/cve/CVE-2021-27216
        CVE-2020-28014  6.1 https://vulners.com/cve/CVE-2020-28014
        CVE-2016-9963   5.9 https://vulners.com/cve/CVE-2016-9963
        PRION:CVE-2020-28014    5.6 https://vulners.com/prion/PRION:CVE-2020-28014
        CVE-2023-51766  5.3 https://vulners.com/cve/CVE-2023-51766
        CHAINGUARD:CVE-2023-42117   5.1 https://vulners.com/cgr/CHAINGUARD:CVE-2023-42117
        CHAINGUARD:CVE-2023-42116   5.1 https://vulners.com/cgr/CHAINGUARD:CVE-2023-42116
        PRION:CVE-2023-51766    5.0 https://vulners.com/prion/PRION:CVE-2023-51766
        PRION:CVE-2022-37451    5.0 https://vulners.com/prion/PRION:CVE-2022-37451
        PRION:CVE-2021-38371    5.0 https://vulners.com/prion/PRION:CVE-2021-38371
        PRION:CVE-2020-28025    5.0 https://vulners.com/prion/PRION:CVE-2020-28025
        PRION:CVE-2020-28023    5.0 https://vulners.com/prion/PRION:CVE-2020-28023
        PRION:CVE-2020-28019    5.0 https://vulners.com/prion/PRION:CVE-2020-28019
        PRION:CVE-2020-12783    5.0 https://vulners.com/prion/PRION:CVE-2020-12783
        CHAINGUARD:CVE-2023-51766   5.0 https://vulners.com/cgr/CHAINGUARD:CVE-2023-51766
        CHAINGUARD:CVE-2023-42118   4.3 https://vulners.com/cgr/CHAINGUARD:CVE-2023-42118
        CVE-2017-1000369    4.0 https://vulners.com/cve/CVE-2017-1000369
        PRION:CVE-2016-9963 2.6 https://vulners.com/prion/PRION:CVE-2016-9963
        CHAINGUARD:CVE-2023-42114   2.6 https://vulners.com/cgr/CHAINGUARD:CVE-2023-42114
        PRION:CVE-2017-1000369  2.1 https://vulners.com/prion/PRION:CVE-2017-1000369
        F5E48F31-294D-5824-9F49-88CB0516C8D6    0.0 https://vulners.com/githubexploit/
F5E48F31-294D-5824-9F49-88CB0516C8D6    *EXPLOIT*
        CNVD-2022-56952 0.0 https://vulners.com/cnvd/CNVD-2022-56952
        CHAINGUARD:GHSA-W6WW-869J-CGM6  0.0 https://vulners.com/cgr/CHAINGUARD:GHSA-W6WW-869J-CGM6
        CHAINGUARD:CVE-2023-42219   0.0 https://vulners.com/cgr/CHAINGUARD:CVE-2023-42219
```

Suggesting Fixes

To address the issue of open ports running vulnerable and outdated services, consider the following suggested fixes:

- **Close Unnecessary Ports:** Identify and close any open ports that are not needed for the normal operation of your services. Only keep essential ports open to minimize the attack surface.
- **Update and Patch Services:** Ensure that the services running on open ports are up to date with the latest versions and security patches. This helps address known vulnerabilities and protect against exploitation.
- **Configure Firewalls:** Use firewalls to control access to open ports. Configure firewall rules to restrict traffic to only trusted sources and required services.
- **Monitor Network Traffic:** Continuously monitor network traffic for signs of suspicious activity on open ports. Implement intrusion detection or prevention systems (IDS/IPS) to identify and block potential threats.

- **Limit Access to Services:** Implement strict access controls on services running on open ports. Use IP whitelisting, VPNs, or other access control mechanisms to restrict who can connect to the services.
- **Implement Security Best Practices:** Secure services running on open ports by following security best practices such as enforcing strong authentication, encryption, and secure configurations.

chowkidar

Vulnerable To Slowloris DDoS Attack

Severity	**High**
CVSS Score	7.5
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability Description

A vulnerability to Slowloris Denial of Service (DoS) attacks occurs when a server or application does not adequately handle partially open connections or slow HTTP requests. Slowloris is a low-bandwidth, application-layer attack designed to consume server resources by making multiple HTTP requests and keeping them open for as long as possible, while sending data very slowly.

Attackers exploit this vulnerability by establishing numerous slow connections to the target server and maintaining them for an extended period. By doing so, Slowloris gradually exhausts the server's available connections, sockets, or memory, preventing legitimate users from establishing new connections.

Potential Risk Associated

- **Service Disruption:** The server's capacity to handle new connections is reduced, potentially leading to service interruptions or outages.
- **Resource Consumption:** Slowloris consumes server resources such as CPU, memory, and sockets, impacting the server's performance and availability.
- **Denial of Service:** Legitimate users may experience slow response times or be unable to access the server altogether due to resource exhaustion caused by Slowloris.

Evidence (POC)

Ports and Services Vulnerable To Slowloris DDoS Attack are

```
80 http
  VULNERABLE:
  Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs:  CVE:CVE-2007-6750
      Slowloris tries to keep many connections to the target web server open and hold
      them open as long as possible.  It accomplishes this by opening connections to
      the target web server and sending a partial request. By doing so, it starves
      the http server's resources causing Denial Of Service.

    Disclosure date: 2009-09-17
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
      http://ha.ckers.org/slowloris/


443 https
  VULNERABLE:
  Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs:  CVE:CVE-2007-6750
      Slowloris tries to keep many connections to the target web server open and hold
      them open as long as possible.  It accomplishes this by opening connections to
```

```
    the target web server and sending a partial request. By doing so, it starves
    the http server's resources causing Denial Of Service.

  Disclosure date: 2009-09-17
  References:
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
    http://ha.ckers.org/slowloris/
```

Suggesting Fixes

To mitigate the risks associated with Slowloris Denial of Service (DoS) attacks, consider implementing the following suggested fixes:

- **Connection Timeouts:** Configure the server to enforce timeouts for connections that remain idle for too long. This can prevent attackers from keeping connections open indefinitely.
- **Rate Limiting:** Implement rate limiting on incoming connections to restrict the number of simultaneous connections or requests from a single IP address. This can help prevent attackers from overwhelming the server with slow connections.
- **Connection Management:** Limit the number of connections each client can establish and control the maximum number of connections per IP address. This can prevent any single client from monopolizing server resources.
- **Application-Layer Firewalls:** Use an application-layer firewall to monitor and filter incoming HTTP requests. These firewalls can detect and block suspicious or malicious requests that exhibit Slowloris-like behavior.
- **Reverse Proxies and Load Balancers:** Deploy a reverse proxy or load balancer to distribute traffic across multiple servers. This can help absorb and mitigate the impact of Slowloris attacks by spreading the load and filtering out malicious requests.
- **Request Limitations:** Set limits on the number of headers, cookies, or query parameters a single request can contain. This can help protect against overly complex or malformed requests used in Slowloris attacks.
- **Web Server Configuration:** Optimize web server configurations to handle slow clients more efficiently, such as adjusting worker processes, thread pooling, and other performance settings.
- **IP Blocking and Blacklisting:** Implement IP blocking or blacklisting for known malicious IP addresses exhibiting Slowloris attack patterns.

chowkidar

Potentially Vulnerable To SWEET32

Severity	**High**
CVSS Score	7.5
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability Description

A system is potentially vulnerable to the SWEET32 attack when it supports certain block cipher modes of operation that use small block sizes, such as 64-bit blocks. The attack targets commonly used block ciphers like DES and 3DES (Triple DES) and takes advantage of the birthday attack to compromise the encryption.

The SWEET32 attack is a practical collision attack that exploits the birthday paradox, allowing attackers to generate collisions within the small block size of the cipher. This attack can lead to the compromise of secure communications by decrypting encrypted data.

Potential Risk Associated

- **Small Block Sizes:** The attack targets block ciphers with small block sizes (e.g., 64 bits) because the smaller the block size, the more feasible it is to generate collisions within the cipher.
- **Long-lived Sessions:** Long-lived sessions with large amounts of encrypted data using vulnerable block ciphers increase the attack surface and the likelihood of an attack succeeding.
- **Exploitation Potential:** Attackers can exploit the SWEET32 vulnerability to intercept and decrypt secure communications, potentially exposing sensitive data such as user credentials, session tokens, or other confidential information.
- **Legacy Cipher Support:** The attack is often a risk when systems support legacy ciphers like DES or 3DES, which are known to be vulnerable due to their small block sizes.

Evidence (POC)

- **CVE-2016-2183 CVE-2016-6329**

Suggesting Fixes

To mitigate the risks associated with the SWEET32 attack and protect against vulnerabilities in block ciphers with small block sizes, such as DES and 3DES, consider implementing the following suggested fixes:

- **Use Modern Block Ciphers:** Replace vulnerable block ciphers such as DES and 3DES with modern and secure block ciphers such as AES. AES uses larger block sizes (e.g., 128 bits) and is not susceptible to the SWEET32 attack.
- **Disable Legacy Cipher Suites:** Ensure that servers and applications do not support legacy or weak cipher suites that include vulnerable block ciphers. Configure systems to use only strong, modern encryption algorithms.
- **Secure Long-lived Sessions:** Limit the use of long-lived sessions when using encryption, as long-lived sessions can increase the risk of the SWEET32 attack. Use short-lived sessions or re-establish secure connections periodically.

chowkidar

Missing Security Headers

Severity	**Medium**
CVSS Score	6.5
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CWE	CWE-525: Missing HTTP Security Headers

Vulnerability Description

Missing security headers refers to the absence of HTTP headers that enhance the security of web applications and protect against common attacks. These headers provide instructions to web browsers on how to handle certain aspects of web pages, such as content type, origin policy, caching behavior, and scripts execution. Common security headers that may be missing include:

- **Content Security Policy (CSP):** Helps prevent cross-site scripting (XSS) and data injection attacks by specifying which sources and types of content are allowed to be loaded and executed on the page.
- **HTTP Strict Transport Security (HSTS):** Forces browsers to connect to the server using a secure HTTPS connection and protects against downgrade attacks.
- **X-Content-Type-Options:** Protects against MIME type sniffing, which can lead to the execution of malicious content.
- **X-Frame-Options:** Prevents clickjacking attacks by controlling whether the page can be embedded within an iframe.
- **X-XSS-Protection:** Provides basic XSS filtering capabilities and instructs the browser to block or sanitize the page if an XSS attack is detected.
- **Referrer-Policy:** Controls the information sent in the Referer header, protecting user privacy by limiting data leakage.

Potential Risk Associated

The impact of having missing or misconfigured security headers can be detrimental to the security and privacy of a web application and its users:

- **Cross-Site Scripting (XSS) Attacks:** Without a properly configured Content Security Policy (CSP) header, the application is more vulnerable to XSS attacks. Attackers can inject malicious scripts into web pages, potentially leading to data theft, session hijacking, or unauthorized actions on behalf of the user.
- **Clickjacking Attacks:** The absence of the X-Frame-Options header allows attackers to embed the web application within an iframe and trick users into clicking on hidden or deceptive content. This can result in unauthorized actions being performed, such as changing user settings or executing transactions.
- **Man-in-the-Middle Attacks:** Missing the HTTP Strict Transport Security (HSTS) header can expose the application to man-in-the-middle attacks, where attackers intercept and manipulate data transmitted between the user and the server. This can lead to data breaches, privacy violations, and tampering with sensitive information.
- **MIME Type Sniffing:** Without the X-Content-Type-Options header set to "nosniff," the browser may attempt to determine the content type of a response based on its content rather than the declared content type. This can lead to unintended content execution or the display of malicious content, posing security risks.
- **Information Leakage:** The absence of the Referrer-Policy header can result in unintentional exposure of user data, such as the URL of the referring page. This can lead to privacy concerns and potential data leakage.
- **Data Integrity Risks:** Without the X-XSS-Protection header, the application lacks basic protection against XSS attacks. This can impact data integrity and user trust in the application's ability to secure their information.

chowkidar

Evidence (POC)

During the scan, the following security headers were missing from the response headers:

- **X-Frame-Options**
- **X-Content-Type-Options**
- **Strict-Transport-Security**
- **Content-Security-Policy**
- **Referrer-Policy**
- **Permissions-Policy**
- **Cross-Origin-Embedder-Policy**
- **Cross-Origin-Resource-Policy**
- **Cross-Origin-Opener-Policy**

Suggesting Fixes

Content Security Policy (CSP)

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control w2at resources the user agent is allowed to load for that page. For example, a page that uploads and displays images could allow images from anywhere, but restrict a form action to a specific endpoint. A properly designed Content Security Policy helps protect a page against a cross-site scripting attack.

```
Content-Security-Policy: default-src 'self'

Content-Security-Policy: default-src 'self' example.com *.example.com

Content-Security-Policy: default-src 'self'; img-src *; media-src example.net; script-src scripts.example.com
```

Strict-Transport-Security (HSTS)

If a website accepts a connection through HTTP and redirects to HTTPS, visitors may initially communicate with the non-encrypted version of the site before being redirected, if, for example, the visitor types http://www.foo.com/ or even just foo.com. This creates an opportunity for a man-in-the-middle attack. The redirect could be exploited to direct visitors to a malicious site instead of the secure version of the original site.
The HTTP Strict Transport Security header informs the browser that it should never load a site using HTTP and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead.

```
Strict-Transport-Security: max-age=<expire-time>

Strict-Transport-Security: max-age=<expire-time>; includeSubDomains

Strict-Transport-Security: max-age=<expire-time>; includeSubDomains; preload
```

X-Content-Type-Options

The X-Content-Type-Options response HTTP header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should be followed and not be changed. The header allows you to avoid MIME type sniffing by saying that the MIME types are deliberately configured.

```
X-Content-Type-Options: nosniff
```

X-Frame-Options

The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a <frame>, <iframe>, <embed> or <object>. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites.

```
X-Frame-Options: DENY
```

chowkidar

```
X-Frame-Options: SAMEORIGIN
```

Referrer-Policy

The Referrer-Policy HTTP header controls how much referrer information (sent with the Referer header) should be included with requests. Aside from the HTTP header, you can set this policy in HTML.

```
Referrer-Policy: no-referrer
Referrer-Policy: no-referrer-when-downgrade
Referrer-Policy: origin
Referrer-Policy: origin-when-cross-origin
Referrer-Policy: same-origin
Referrer-Policy: strict-origin
Referrer-Policy: strict-origin-when-cross-origin
Referrer-Policy: unsafe-url
```

Permissions Policy

Permissions Policy provides mechanisms for web developers to explicitly declare what functionality can and cannot be used on a website. You define a set of "policies" that restrict what APIs the site's code can access or modify the browser's default behavior for certain features. This allows you to enforce best practices, even as the codebase evolves — as well as more safely compose third-party content.
Permissions Policy is similar to Content Security Policy but controls features instead of security behavior.

```
Permissions-Policy: <directive>=<allowlist>
Permissions-Policy: geolocation=()
Permissions-Policy: geolocation=(self "https://a.example.com" "https://b.example.com")
Permissions-Policy: picture-in-picture=(), geolocation=(self https://example.com), camera=*;
```

Cross-Origin-Embedder-Policy (COEP)

The HTTP Cross-Origin-Embedder-Policy (COEP) response header configures embedding cross-origin resources into the document.

```
Cross-Origin-Embedder-Policy: unsafe-none | require-corp | credentialless
```

Cross-Origin Resource Policy (CORP)

Cross-Origin Resource Policy is a policy set by the Cross-Origin-Resource-Policy HTTP header that lets websites and applications opt in to protection against certain requests from other origins (such as those issued with elements like <script> and <img>), to mitigate speculative side-channel attacks, like Spectre, as well as Cross-Site Script Inclusion attacks.

```
Cross-Origin-Resource-Policy: same-site | same-origin | cross-origin
```

Cross-Origin-Opener-Policy (COOP)

The HTTP Cross-Origin-Opener-Policy (COOP) response header allows you to ensure a top-level document does not share a browsing context group with cross-origin documents.
COOP will process-isolate your document and potential attackers can't access your global object if they were to open it in a popup, preventing a set of cross-origin attacks dubbed XS-Leaks.

```
Cross-Origin-Opener-Policy: unsafe-none
Cross-Origin-Opener-Policy: same-origin-allow-popups
```

chowkidar

Cross-Origin-Opener-Policy: same-origin

chowkidar

Non Compliant TLS Enabled

Severity	**Medium**
CVSS Score	6.5
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability Description

A system is potentially vulnerable due to non-compliant TLS configurations when it uses outdated, insecure, or incorrectly implemented TLS protocols and cipher suites. TLS (Transport Layer Security) is the standard protocol for securing data in transit, but its effectiveness relies on using modern and compliant configurations.

A non-compliant TLS configuration can occur in several ways:

- **Outdated Protocols:** The system may use older versions of TLS (e.g., TLS 1.0 or TLS 1.1), which have known vulnerabilities and are considered insecure. Modern protocols like TLS 1.2 and TLS 1.3 are more secure and should be used instead.
- **Weak Cipher Suites:** The system may support weak or deprecated cipher suites that use vulnerable encryption methods (e.g., RC4) or small key lengths. These cipher suites can be exploited by attackers to decrypt communications or perform other attacks.
- **Improper Configurations:** TLS configurations that do not adhere to security best practices, such as using default settings, missing security headers, or improper certificate management, can leave the system exposed to various attacks.
- **Lack of Forward Secrecy:** The system may lack support for cipher suites that provide forward secrecy, which ensures that session keys are not compromised even if the private key is exposed.
- **Insecure Certificate Management:** The system may use weak or self-signed certificates, or may not properly verify certificates, exposing it to man-in-the-middle attacks.

Potential Risk Associated

- **Data Interception and Decryption:** Attackers can exploit vulnerabilities in non-compliant TLS configurations to intercept and decrypt encrypted communications, exposing sensitive information.
- **Man-in-the-Middle Attacks:** Weak or improperly configured TLS can allow attackers to perform man-in-the-middle attacks, intercepting and manipulating data in transit.
- **Loss of Confidentiality and Integrity:** Non-compliant TLS configurations can compromise the confidentiality and integrity of communications, leading to data breaches and privacy violations.
- **Compliance Violations:** Using non-compliant TLS configurations may result in violations of data protection regulations and industry standards, potentially leading to legal and financial consequences.

Evidence (POC)

The following non-compliant TLS versions are enabled:

- **TLS1**
- **TLS1_1**

Suggesting Fixes

To mitigate the risks associated with enabling non-compliant TLS versions, consider implementing the following suggested fixes:

- **Disable Outdated TLS Versions:** Disable support for outdated TLS versions such as TLS 1.0 and TLS 1.1 on servers and clients. This ensures that only secure, modern TLS versions like TLS 1.2 and TLS 1.3 are used.
- **Use Strong Cipher Suites:** Configure servers to use strong, modern cipher suites that offer secure encryption and authentication. Avoid weak or deprecated cipher suites that may pose security risks.

chowkidar

No DMARC Record Found

Severity	**Medium**
CVSS Score	5.9
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE	CWE-290: Authentication Bypass by Spoofing

Vulnerability Description

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a protocol that builds on SPF and DKIM (DomainKeys Identified Mail) to improve email security. It provides a way for domain owners to specify how emails that fail authentication checks should be handled. If no DMARC record is found, domain owners are unable to enforce policies for handling unauthenticated emails and cannot receive feedback on email authentication issues. This absence increases the risk of email spoofing and phishing attacks, as attackers can exploit the lack of DMARC policy to impersonate the domain and deceive recipients.

Potential Risk Associated

- **Increased Phishing Risk:** Without DMARC, it’s harder to prevent malicious actors from sending phishing emails that appear to come from your domain.
- **Lack of Visibility:** The absence of DMARC prevents the collection of reports on email authentication issues, hindering the domain owner’s ability to monitor and address email abuse.
- **Reputation Damage:** The domain's reputation may suffer if attackers successfully impersonate it, leading to a loss of trust among recipients.

Evidence (POC)

The scanner did not find any DMARC record for this domain:

- **your-scope-url.com**

Suggesting Fixes

To mitigate this vulnerability, implement a DMARC record for your domain. Add a **TXT** record to your DNS zone that specifies the desired DMARC policy. The record should include instructions on how to handle emails that fail authentication checks and how to report them.

chowkidar

Vulnerable To Diffie-Hellman Key Exchange Attack

Severity	**Medium**
CVSS Score	5.9
CVSS String	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE	CWE-324: Use of a Key Exchange Without Entity Authentication

Vulnerability Description

Vulnerability to a Diffie-Hellman key exchange attack occurs when the Diffie-Hellman key exchange process is implemented using weak or insecure parameters, making it susceptible to cryptographic attacks such as the Logjam attack. Diffie-Hellman key exchange is a method used to establish a shared secret between two parties over an insecure communication channel.

- **Man-in-the-Middle (MitM) Attacks:** An attacker can intercept and manipulate the key exchange process, inserting themselves between the two parties to establish two separate secure channels. This allows the attacker to decrypt, modify, or inject data as it passes through them.
- **Weak Parameters:** The use of weak or commonly used parameters (e.g., small or non-random prime numbers) in the Diffie-Hellman key exchange process can allow attackers to crack the key exchange and compromise the shared secret.
- **Insufficient Key Sizes:** Using insufficiently large key sizes can make the Diffie-Hellman key exchange vulnerable to brute-force or other cryptographic attacks.

Potential Risk Associated

- **Data Interception:** Attackers can eavesdrop on encrypted communications, intercepting sensitive information such as authentication credentials, personal data, or financial information.
- **Data Manipulation:** Attackers may manipulate the data being transmitted between parties, leading to data corruption or unauthorized changes.
- **Loss of Confidentiality:** By breaking the key exchange process, attackers can gain access to the shared secret and decrypt communications, resulting in the loss of confidentiality.
- **Loss of Integrity:** Attackers can modify data in transit, compromising the integrity of the communication and potentially leading to further attacks.

Evidence (POC)

Ports and Services Vulnerable To Diffie-Hellman Key Exchange Attack are

```
21 ftp
  VULNERABLE:
  Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
    State: VULNERABLE
      Transport Layer Security (TLS) services that use anonymous
      Diffie-Hellman key exchange only provide protection against passive
      eavesdropping, and are vulnerable to active man-in-the-middle attacks
      which could completely compromise the confidentiality and integrity
      of any data exchanged over the resulting session.
    Check results:
      ANONYMOUS DH GROUP 1
            Cipher Suite: TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
            Modulus Type: Safe prime
            Modulus Source: Unknown/Custom-generated
            Modulus Length: 2048
```

```
            Generator Length: 8
            Public Key Length: 2048
    References:
      https://www.ietf.org/rfc/rfc2246.txt


110 pop3
  VULNERABLE:
  Diffie-Hellman Key Exchange Insufficient Group Strength
    State: VULNERABLE
      Transport Layer Security (TLS) services that use Diffie-Hellman groups
      of insufficient strength, especially those using one of a few commonly
      shared groups, may be susceptible to passive eavesdropping attacks.
    Check results:
      WEAK DH GROUP 1
            Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
            Modulus Type: Safe prime
            Modulus Source: Unknown/Custom-generated
            Modulus Length: 1024
            Generator Length: 8
            Public Key Length: 1024
    References:
      https://weakdh.org


143 imap
  VULNERABLE:
  Diffie-Hellman Key Exchange Insufficient Group Strength
    State: VULNERABLE
      Transport Layer Security (TLS) services that use Diffie-Hellman groups
      of insufficient strength, especially those using one of a few commonly
      shared groups, may be susceptible to passive eavesdropping attacks.
    Check results:
      WEAK DH GROUP 1
            Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
            Modulus Type: Safe prime
            Modulus Source: Unknown/Custom-generated
            Modulus Length: 1024
            Generator Length: 8
            Public Key Length: 1024
    References:
      https://weakdh.org


993 imaps
  VULNERABLE:
  Diffie-Hellman Key Exchange Insufficient Group Strength
    State: VULNERABLE
      Transport Layer Security (TLS) services that use Diffie-Hellman groups
      of insufficient strength, especially those using one of a few commonly
      shared groups, may be susceptible to passive eavesdropping attacks.
    Check results:
      WEAK DH GROUP 1
            Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
            Modulus Type: Safe prime
            Modulus Source: Unknown/Custom-generated
            Modulus Length: 1024
            Generator Length: 8
            Public Key Length: 1024
    References:
      https://weakdh.org
```

```
995 pop3s
   VULNERABLE:
   Diffie-Hellman Key Exchange Insufficient Group Strength
     State: VULNERABLE
       Transport Layer Security (TLS) services that use Diffie-Hellman groups
       of insufficient strength, especially those using one of a few commonly
       shared groups, may be susceptible to passive eavesdropping attacks.
     Check results:
       WEAK DH GROUP 1
             Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
             Modulus Type: Safe prime
             Modulus Source: Unknown/Custom-generated
             Modulus Length: 1024
             Generator Length: 8
             Public Key Length: 1024
     References:
       https://weakdh.org
```

Suggesting Fixes

To mitigate these risks, one should use secure and updated Diffie-Hellman key exchange implementations, avoid using commonly used or weak parameters, and opt for sufficiently large key sizes. Additionally, using other cryptographic protocols, such as Elliptic Curve Diffie-Hellman (ECDH), can provide stronger security and protection against such attacks.

chowkidar

Vulnerable to Lucky13

Severity	**Medium**
CVSS Score	5.6
CVSS String	AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
CWE	CWE-208: Observable Timing Discrepancy

Vulnerability Description

A system is potentially vulnerable due to non-compliant TLS configurations when it uses outdated, insecure, or incorrectly implemented TLS protocols and cipher suites. TLS (Transport Layer Security) is the standard protocol for securing data in transit, but its effectiveness relies on using modern and compliant configurations.

A non-compliant TLS configuration can occur in several ways:

- **Outdated Protocols:** The system may use older versions of TLS (e.g., TLS 1.0 or TLS 1.1), which have known vulnerabilities and are considered insecure. Modern protocols like TLS 1.2 and TLS 1.3 are more secure and should be used instead.
- **Weak Cipher Suites:** The system may support weak or deprecated cipher suites that use vulnerable encryption methods (e.g., RC4) or small key lengths. These cipher suites can be exploited by attackers to decrypt communications or perform other attacks.
- **Improper Configurations:** TLS configurations that do not adhere to security best practices, such as using default settings, missing security headers, or improper certificate management, can leave the system exposed to various attacks.
- **Lack of Forward Secrecy:** The system may lack support for cipher suites that provide forward secrecy, which ensures that session keys are not compromised even if the private key is exposed.
- **Insecure Certificate Management:** The system may use weak or self-signed certificates, or may not properly verify certificates, exposing it to man-in-the-middle attacks.

Potential Risk Associated

The impact of vulnerability to the Lucky13 attack can be significant due to its ability to compromise the confidentiality and integrity of encrypted data:

- **Decryption of Encrypted Data:** Attackers can exploit the Lucky13 vulnerability to decrypt encrypted data, potentially exposing sensitive information such as session cookies, user credentials, financial data, or other confidential information.
- **Loss of Confidentiality:** The successful decryption of data compromises the confidentiality of secure communications, leading to data breaches and exposure of sensitive information.
- **Session Hijacking:** Attackers can hijack user sessions by decrypting session cookies, potentially gaining unauthorized access to accounts and performing actions on behalf of the user.
- **Man-in-the-Middle Attacks:** The attack can involve intercepting encrypted communications, allowing attackers to perform man-in-the-middle attacks and manipulate data in transit.
- **Privacy Violations:** The exposure of encrypted data can lead to privacy violations, affecting both individual users and organizations.

Evidence (POC)

Here is a list of all the weak cipher suites used by the server:

107.167.23.66

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Suggesting Fixes

To mitigate the risks associated with the Lucky13 attack and protect against vulnerabilities in TLS with CBC mode encryption, consider implementing the following suggested fixes:

- **Upgrade to Modern TLS Versions:** Use TLS 1.2 or later, which includes stronger security features and improved handling of padding verification, reducing the risk of timing attacks.
- **Use Authenticated Encryption Modes:** Choose cipher suites that use authenticated encryption modes such as AES-GCM (Galois/Counter Mode) or AES-CCM (Counter with CBC-MAC) instead of CBC mode. These modes provide confidentiality and integrity protection and are not vulnerable to Lucky13.
- **Disable Older TLS Versions:** Disable support for older TLS versions such as TLS 1.0 and 1.1, which may use vulnerable encryption modes and have other weaknesses.
- **Timing Obfuscation:** Implement timing obfuscation techniques in the padding verification process to reduce observable timing discrepancies. This can make it more difficult for attackers to exploit timing differences.

chowkidar

Banner Grabbing

Severity	**Medium**
CVSS Score	5.3
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE	CWE-213: Exposed Information through Server Headers

Vulnerability Description

When an HTTP response includes a server header that discloses the server software and its version, it provides attackers with valuable information about the underlying infrastructure. This disclosure can help attackers tailor their attacks to target known vulnerabilities associated with the specific server software version. Such information may include the type of server (e.g., Apache, Nginx, or IIS) and its exact version number.

Attackers can use this information for:

- **Targeted Attacks:** Knowing the server software and its version allows attackers to research known vulnerabilities and exploits specific to that version. This can lead to targeted attacks such as buffer overflow, code execution, or denial-of-service attacks.
- **Reconnaissance:** Server header information can provide attackers with insights into the technology stack of the application, enabling them to map out the network infrastructure and identify potential attack vectors.
- **Fingerprinting:** Attackers can use server version information for fingerprinting purposes, gathering details about the server environment to inform their attack strategies.

Potential Risk Associated

The impact of banner grabbing can be significant, especially when attackers obtain sensitive information about a server's configuration and software versions:

- **Targeted Attacks:** Banner grabbing provides attackers with details about the server's software, including type and version. Attackers can use this information to tailor their attacks to exploit known vulnerabilities specific to the server software version.
- **Reconnaissance and Mapping:** Attackers can gather information about the server and its technology stack, aiding in reconnaissance and mapping the network infrastructure. This information can be used to identify potential attack vectors and weaknesses in the network.
- **Exploitation of Known Vulnerabilities:** By knowing the server's software and version, attackers can look up known vulnerabilities in vulnerability databases and attempt to exploit them. This can lead to unauthorized access, data breaches, and other forms of exploitation.
- **Increased Risk of Other Attacks:** Knowing the server's software and version can provide attackers with insights into potential weaknesses that could be exploited through other attack methods, such as cross-site scripting (XSS), cross-site request forgery (CSRF), or SQL injection.
- **Information Leakage:** Banner grabbing may reveal other sensitive information, such as the server's operating system, configuration settings, or internal network details. This information can aid attackers in crafting more precise and effective attacks.

Evidence (POC)

The headers revealing the server version was discovered

- **X-Powered-By: PHP/5.4.45**

Suggesting Fixes

To address the issue of a header revealing the server version, consider the following suggested fixes:

- **Remove or Obfuscate the Server Header:** Configure the server to remove or modify the server header in HTTP responses. This can help prevent attackers from easily identifying the server software and its version.
- **Server Configuration:** Most web servers allow you to customize or disable the server header. Refer to your server's documentation (e.g., Apache, Nginx, IIS) to configure the server appropriately.
- **Implement a Web Application Firewall (WAF):** A WAF can help filter and block suspicious requests and responses, potentially providing an additional layer of protection and masking certain server information.

chowkidar

Directory Listing Enabled

Severity	**Medium**
CVSS Score	5.3
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE	CWE-548: Exposure of Information Through Directory Listing

Vulnerability Description

Web servers can be configured to automatically list the contents of directories that do not have an index page present. This can aid an attacker by enabling them to quickly identify the resources at a given path, and proceed directly to analyzing and attacking those resources. It particularly increases the exposure of sensitive files within the directory that are not intended to be accessible to users, such as temporary files and crash dumps.

Directory listings themselves do not necessarily constitute a security vulnerability. Any sensitive resources within the web root should in any case be properly access-controlled, and should not be accessible by an unauthorized party who happens to know or guess the URL. Even when directory listings are disabled, an attacker may guess the location of sensitive files using automated tools.

Potential Risk Associated

- **Sensitive Files:** Directory listings can expose files that contain sensitive information, such as configuration files, backup files, or private documents. These files might include credentials, internal communications, or other confidential data.
- **Discovery of Hidden Resources:** Attackers can discover hidden resources that are not linked or indexed, such as admin panels, test files, or deprecated scripts.
- **Identification of Vulnerable Files:** Attackers can identify and exploit files with known vulnerabilities (e.g., outdated scripts with security flaws).
- **Website Structure Insight:** Attackers can gain a comprehensive understanding of the website's directory structure, making it easier to identify important files and directories.

Evidence (POC)

Discovering endpoints can occur through techniques such as:

- **Web Crawling:** Scanning the application's publicly accessible URLs and directories to discover available endpoints.
- **Brute Forcing:** Systematically trying different URL patterns or parameter combinations to uncover hidden endpoints.
- **Reverse Engineering:** Analyzing client-side code, such as JavaScript files, or network traffic to identify and map application endpoints.

- **https://your-scope-url.com/includes/**
- **https://your-scope-url.com/js/**
- **https://your-scope-url.com/lib/**

Suggesting Fixes

There is not usually any good reason to provide directory listings, and disabling them may place additional hurdles in the path of an attacker. This can normally be achieved in two ways:

- Configure your web server to prevent directory listings for all paths beneath the web root;

- Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing.
- Disable directory listing in the web server configuration (e.g., using .htaccess for Apache or nginx.conf for NGINX).
- Implement proper access controls to restrict unauthorized access to directories.

For **Apache** web server, disabling directory listing can be achieved by adding the following line to the .htaccess file or the server configuration:

```
Options -Indexes
```

For **NGINX**, the following directive can be added to the server block:

```
autoindex off;
```

chowkidar

Potentially Vulnerable To LOGJAM

Severity	Low
CVSS Score	3.7
CVSS String	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE	CWE-310: Cryptographic Issues

Vulnerability Description

A system is potentially vulnerable to the Logjam attack when it supports weak Diffie-Hellman (DH) key exchange parameters, particularly small or non-random prime numbers. Logjam is a cryptographic attack that targets the Diffie-Hellman key exchange protocol and allows attackers to downgrade secure connections and break the encryption to intercept and manipulate data.

The attack leverages a vulnerability in the key exchange process to downgrade secure connections to use weak DH parameters. When a server supports weak DH groups, attackers can perform a man-in-the-middle attack to downgrade the connection and exploit the key exchange process. This can lead to the compromise of secure communications.

Potential Risk Associated

- **Weak DH Parameters:** The attack targets the use of small or non-random prime numbers in the DH key exchange process, which are easier to factorize and compromise.
- **Man-in-the-Middle Attacks:** Attackers can perform a man-in-the-middle attack to intercept and manipulate the key exchange process, downgrading the connection to use weak DH parameters.
- **Compromise of Secure Communications:** By compromising the key exchange, attackers can decrypt secure communications, exposing sensitive data such as encryption keys, session tokens, or user credentials.
- **Downgrade Attacks:** Attackers can force connections to use weak DH parameters even if the client and server support stronger parameters.

Evidence (POC)

None

- **CVE-2015-4000**

Suggesting Fixes

To mitigate the risks associated with the Logjam attack and protect against vulnerabilities in Diffie-Hellman (DH) key exchange, consider implementing the following suggested fixes:

- **Use Strong DH Parameters:** Ensure that the server supports only secure and strong Diffie-Hellman parameters, such as large prime numbers (at least 2048 bits). This makes it more difficult for attackers to compromise the key exchange.
- **Upgrade to Modern Cryptographic Protocols:** Use modern cryptographic protocols such as TLS 1.2 or TLS 1.3, which use stronger encryption algorithms and do not support weak DH parameters.
- **Disable Export-Grade Cipher Suites:** Avoid using export-grade or weak cipher suites that may use small DH parameters. Modern servers should use secure cipher suites and avoid any that allow for insecure key exchanges.
- **Secure DH Parameter Generation:** Generate and use secure, large, and safe prime numbers for DH parameters. Avoid using commonly used or publicly known prime numbers.

- **Monitor and Audit:** Continuously monitor and audit your cryptographic configurations to ensure compliance with security best practices and prevent the use of weak DH parameters.
- **Configure Server Security Settings:** Check and update server configurations to ensure they do not support legacy protocols or insecure DH parameters. This may involve updating software, adjusting configurations, and reviewing cipher suite preferences.
- **Implement Certificate Pinning:** Use certificate pinning to ensure the integrity of SSL/TLS connections, protecting against man-in-the-middle attacks and downgrades.

chowkidar

Review Open Ports

Severity	Low
CVSS Score	3.7
CVSS String	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE	CWE-1125: Excessive Attack Surface

Vulnerability Description

Open ports refer to network ports on a server or device that are accessible to the outside world. These ports allow incoming and outgoing communication for specific services and protocols (e.g., HTTP on port 80, HTTPS on port 443, SSH on port 22). While open ports are necessary for legitimate network services and applications to function, they can also pose security risks if not properly managed.

When ports are left open, particularly those not needed for normal operations, it can create vulnerabilities in the network or server. Attackers may exploit these open ports to gain unauthorized access, compromise systems, or launch attacks.

Potential Risk Associated

- **Unrestricted Access:** Open ports can provide attackers with direct access to services running on the server, potentially bypassing other network defenses.
- **Vulnerability Exploitation:** Attackers may attempt to exploit vulnerabilities in services running on open ports, such as outdated software or misconfigured services, leading to unauthorized access or service disruptions.
- **Network Reconnaissance:** Open ports can reveal information about the types of services and software running on the server, aiding attackers in mapping the network and planning targeted attacks.
- **Denial of Service (DoS) Attacks:** Open ports can be targeted with a high volume of traffic, potentially causing service disruptions and server overload.
- **Data Breaches:** Unsecured open ports can provide attackers with a pathway to access sensitive data stored on the server or transmitted through network communications.

Evidence (POC)

The following ports are open

PORTS	SERVICES	VERSION
21	ftp	ProFTPD 1.3.5b
22	tcpwrapped	
26	rsftp	
53	domain	ISC BIND 9.8.2rc1
80	http	Apache httpd
110	pop3	Dovecot pop3d
143	imap	Dovecot imapd

PORTS	SERVICES	VERSION
443	http	Apache httpd
465	smtp	Exim smtpd 4.87
993	imap	Dovecot imapd
995	pop3	Dovecot pop3d
2077	tsrmagt	
2078	http	cPanel httpd
2082	http	cPanel httpd 11.56.0.52
2083	http	cPanel httpd 11.56.0.52
2087	http	cPanel httpd 11.56.0.52
2095	http	cPanel httpd 11.56.0.52
2096	http	cPanel httpd 11.56.0.52
3306	mysql	MySQL 5.5.52-cll
8080	http-proxy	

Suggesting Fixes

To address the risks associated with open ports, consider the following suggested fixes:

- **Close Unnecessary Ports:** Review the open ports on your servers and close any that are not necessary for the normal operation of your services. Only keep ports open that are required for specific services and applications.
- **Firewall Configuration:** Use firewalls to control access to open ports. Configure firewall rules to restrict incoming and outgoing traffic to only trusted sources and required services.
- **Access Control:** Implement strict access controls on open ports, limiting access to authorized users and trusted networks. Use methods such as VPNs or IP whitelisting to secure access to sensitive services.
- **Port Scanning:** Regularly perform port scans on your network to identify open ports and ensure that only necessary ports remain open. Identify any unexpected or unauthorized open ports and investigate their causes.

chowkidar

Potentially Vulnerable To BEAST

Severity	Low
CVSS Score	3.7
CVSS String	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability Description

A system is potentially vulnerable to the BEAST (Browser Exploit Against SSL/TLS) attack when it uses the TLS 1.0 or SSL 3.0 protocols with cipher block chaining (CBC) mode encryption. BEAST is a cryptographic attack that exploits a vulnerability in the way the protocols handle CBC mode, allowing attackers to decrypt encrypted data and potentially expose sensitive information.

The attack works by intercepting encrypted communications between a client and server and manipulating the initialization vector (IV) of the CBC mode to decrypt data one byte at a time. By observing the decrypted data, attackers can recover plaintext information from the encrypted messages.

Potential Risk Associated

The impact of vulnerability to the BEAST (Browser Exploit Against SSL/TLS) attack can be significant:

- **Decryption of Encrypted Data:** Attackers can exploit the BEAST vulnerability to decrypt encrypted communications, exposing sensitive information such as session cookies, user credentials, or financial data.
- **Session Hijacking:** By decrypting session cookies, attackers can hijack user sessions and gain unauthorized access to accounts, potentially compromising user data and activities.
- **Loss of Confidentiality:** Successful exploitation of the BEAST attack compromises the confidentiality of encrypted communications, leading to data breaches and exposure of sensitive information.
- **Man-in-the-Middle Attacks:** Attackers can perform man-in-the-middle attacks by intercepting and manipulating data in transit. This can lead to data tampering or injection of malicious content.
- **Privacy Violations:** The exposure of encrypted data can lead to privacy violations, affecting both individual users and organizations.

Evidence (POC)

- **CVE-2011-3389**

Suggesting Fixes

To mitigate the risks associated with the BEAST (Browser Exploit Against SSL/TLS) attack and protect against vulnerabilities in TLS 1.0 or SSL 3.0 with cipher block chaining (CBC) mode encryption, consider implementing the following suggested fixes:

- **Upgrade to Modern Encryption Protocols:** Transition to TLS 1.2 or later protocols that do not support the weak encryption methods vulnerable to BEAST. Modern protocols offer improved security features and are not susceptible to the BEAST attack.
- **Avoid CBC Mode in Encryption:** Use encryption modes that are resistant to the BEAST attack, such as Galois/Counter Mode (GCM) or Counter Mode (CTR), instead of CBC mode.
- **Disable SSL 3.0 and TLS 1.0:** Disable outdated SSL 3.0 and TLS 1.0 protocols on servers and clients. Ensure that your servers and clients support only TLS 1.2 or later.

- **Configure Secure Cipher Suites:** Choose and prioritize strong cipher suites for SSL/TLS connections that use modern encryption modes. Avoid weak or deprecated cipher suites that support vulnerable encryption methods.
- **Review Third-Party Dependencies:** If your systems rely on third-party services or dependencies, ensure they adhere to security best practices and do not use vulnerable protocols or encryption methods.

chowkidar

Vulnerable To Poodle SSLv3 Attack

Severity	Low
CVSS Score	3.4
CVSS String	AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N
CWE	CWE-319: Cleartext Transmission of Sensitive Information

Vulnerability Description

The vulnerability to the POODLE (Padding Oracle On Downgraded Legacy Encryption) SSLv3 attack occurs when a server or client supports the outdated SSLv3 encryption protocol. The POODLE attack exploits a design flaw in the SSLv3 protocol's padding mechanism, allowing attackers to decrypt encrypted communications and access sensitive information.

In the POODLE attack, an attacker intercepts encrypted data between a client and server and manipulates the data to create errors in the decryption process. By observing how the server responds to these errors, the attacker can use a padding oracle attack to gradually recover the plaintext data from the encrypted messages.

Key points about the POODLE SSLv3 vulnerability:

- **Legacy Protocol:** SSLv3 is an outdated and insecure protocol that should no longer be used due to its susceptibility to attacks like POODLE.
- **Decryption of Encrypted Data:** Attackers can exploit the POODLE vulnerability to decrypt encrypted communications and gain access to sensitive information such as usernames, passwords, session cookies, and other confidential data.
- **Man-in-the-Middle Attack:** The POODLE attack is a type of man-in-the-middle attack that involves intercepting and manipulating data between a client and server.
- **Downgrade Attack:** Attackers can force a downgrade of the encryption protocol from a more secure version (e.g., TLS 1.2) to SSLv3 to exploit the vulnerability.

Potential Risk Associated

The impact of vulnerability to the POODLE (Padding Oracle On Downgraded Legacy Encryption) SSLv3 attack can be significant:

- **Decryption of Encrypted Data:** Attackers can exploit the POODLE vulnerability to decrypt encrypted communications, exposing sensitive data such as usernames, passwords, session cookies, financial information, or other confidential data.
- **Man-in-the-Middle Attacks:** The POODLE attack involves intercepting and manipulating data between a client and server, allowing attackers to perform man-in-the-middle attacks. This can lead to data tampering, interception, or redirection of traffic.
- **Session Hijacking:** By decrypting session cookies and other session-related information, attackers can hijack user sessions, gaining unauthorized access to accounts and performing actions on behalf of the user.
- **Loss of Confidentiality:** Successful exploitation of the POODLE attack compromises the confidentiality of encrypted communications, leading to data breaches and exposure of sensitive information.
- **Compliance Violations:** Using the outdated SSLv3 protocol may violate data protection regulations or industry standards that require the use of up-to-date encryption protocols. This can result in legal consequences, fines, or penalties for non-compliance.

Evidence (POC)

Ports and Services Vulnerable To Poodle SSLv3 Attack are

```
21 ftp
  VULNERABLE:
  SSL POODLE information leak
    State: LIKELY VULNERABLE
    IDs:  BID:70574  CVE:CVE-2014-3566
          The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
          products, uses nondeterministic CBC padding, which makes it easier
          for man-in-the-middle attackers to obtain cleartext data via a
          padding-oracle attack, aka the "POODLE" issue.
    Disclosure date: 2014-10-14
    Check results:
      TLS_RSA_WITH_AES_128_CBC_SHA
      TLS_FALLBACK_SCSV properly implemented
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
      https://www.openssl.org/~bodo/ssl-poodle.pdf
      https://www.securityfocus.com/bid/70574
      https://www.imperialviolet.org/2014/10/14/poodle.html
```

Suggesting Fixes

To mitigate the risks associated with vulnerability to the POODLE (Padding Oracle On Downgraded Legacy Encryption) SSLv3 attack, consider the following suggested fixes:

- **Disable SSLv3 Support:** Remove support for the SSLv3 encryption protocol in servers and clients. This ensures that connections use more secure and modern encryption protocols such as TLS 1.2 or later.
- **Use Secure Protocols:** Enable and prioritize the use of modern and secure encryption protocols, such as TLS 1.2 or TLS 1.3, which are not susceptible to the POODLE attack.
- **Update Software and Libraries:** Ensure that server software, libraries, and clients are up to date with the latest security patches. This helps protect against known vulnerabilities and ensures the use of secure protocols.
- **Configure Cipher Suites:** Configure secure cipher suites for SSL/TLS connections. Use strong encryption algorithms and avoid weak or deprecated cipher suites.

chowkidar

Endpoints Discovered

Severity	**Info**
CVSS Score	0.0
CVSS String	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability Description

Endpoints discovered refer to the process where attackers identify various API or web application endpoints that are publicly accessible or exposed. These endpoints can reveal valuable information about the application's structure, functionality, and available services. Attackers can leverage this information to gain insights into how the application works, what data it handles, and potential vulnerabilities in the exposed endpoints. Once endpoints are discovered, attackers can use this information to probe for vulnerabilities, exploit security weaknesses, or manipulate the application's data and behavior.

Potential Risk Associated

The impact of discovering endpoints in an application can vary depending on the level of exposure and the sensitivity of the endpoints:

- **Unauthorized Access:** Attackers who discover endpoints may attempt to access them directly, potentially bypassing authentication or authorization mechanisms. This can lead to unauthorized access to sensitive data, functionalities, or resources.
- **Reconnaissance:** Knowledge of endpoints can provide attackers with valuable information about the structure and functionality of an application. This can aid in planning and executing targeted attacks.
- **Exploitation of Vulnerabilities:** If the endpoints have vulnerabilities, attackers may exploit them to gain access to the application or its data. This can lead to data breaches, account takeovers, or other forms of exploitation.
- **Manipulation of Data:** Attackers may use discovered endpoints to manipulate data within the application. This can include altering records, injecting malicious data, or disrupting normal operations.

Evidence (POC)

Discovering endpoints can occur through techniques such as:

- **Web Crawling:** Scanning the application's publicly accessible URLs and directories to discover available endpoints.
- **Brute Forcing:** Systematically trying different URL patterns or parameter combinations to uncover hidden endpoints.
- **Reverse Engineering:** Analyzing client-side code, such as JavaScript files, or network traffic to identify and map application endpoints.

- **https://your-scope-url.com/404.html**
- **https://your-scope-url.com/adv.html**
- **https://your-scope-url.com/blog/wp-login.php**
- **https://your-scope-url.com/blog/**
- **https://your-scope-url.com/config.php**
- **https://your-scope-url.com/contact_us.html**
- **https://your-scope-url.com/db.php**
- **https://your-scope-url.com/dump.sql**
- **https://your-scope-url.com/favicon.ico**
- **https://your-scope-url.com/gallery.php**
- **https://your-scope-url.com/htaccess.txt**

- **https://your-scope-url.com/images/**
- **https://your-scope-url.com/includes/**
- **https://your-scope-url.com/java-sys/**
- **https://your-scope-url.com/js/**
- **https://your-scope-url.com/lib/**
- **https://your-scope-url.com/index2.php**
- **https://your-scope-url.com/mailman/listinfo**
- **https://your-scope-url.com/movies**
- **https://your-scope-url.com/search.php**
- **https://your-scope-url.com/sitemap.xml**

Suggesting Fixes

To address the risks associated with the discovery of endpoints, organizations should implement the following suggested fixes:

- **Proper Authentication and Authorization:** Secure endpoints by requiring authentication and authorization checks for all requests. Use role-based access control (RBAC) to limit access to endpoints based on user roles and permissions.
- **Rate Limiting and Throttling:** Implement rate limiting and request throttling to prevent attackers from exploiting endpoints through brute-force attacks or denial-of-service (DoS) attacks.
- **Input Validation and Output Encoding:** Validate all input data to ensure it meets expected criteria and avoid injection attacks. Encode output data to protect against cross-site scripting (XSS) and other injection attacks.
- **Secure API Design:** Follow best practices for secure API design, such as using HTTPS for all communication, avoiding unnecessary data exposure, and using secure tokens for authentication.
- **Minimize Endpoint Exposure:** Limit the number of publicly accessible endpoints to only those necessary for the application's functionality. Hide internal or administrative endpoints behind secure firewalls or VPNs.