Flan Scan Report

January 22, 2025

Summary

Flan Scan ran a network vulnerability scan with the following Nmap command on Sun Jan 19 22:23:59 2025UTC.

```
nmap -sV -oX <output-file> -oN - -v1 --script=vulners/vulners.nse
```

To find out what IPs were scanned see the end of this report.

Services with Vulnerabilities

1 OpenSSH 9.2p1 Debian 2+deb12u4 (cpe:/a:openbsd:openssh:9.2p1) (cpe:/o:linux:linux_ker

95499236-C9FE-56A6-9D7D-E943A24B633A High (10.0) link

Summary:

2C119FFA-ECE0-5E14-A4A4-354A2C38071A High (10.0) link

Summary:

CVE-2023-38408 High (9.8) link

Summary:The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

CVE-2023-28531 High (9.8) link

Summary:ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.

B8190CDB-3EB9-5631-9828-8064A1575B23 High (9.8) link

Summary:

8FC9C5AB-3968-5F3C-825E-E8DB5379A623 High (9.8) link

Summary:

8AD01159-548E-546E-AA87-2DE89F3927EC High (9.8) link
Summary:

887EB570-27D3-11EE-ADBA-C80AA9043978 High (9.8) link
Summary:

5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A High (9.8) link
Summary:

33D623F7-98E0-5F75-80FA-81AA666D1340 High (9.8) link
Summary:

0221525F-07F5-5790-912D-F4B9E2D1B587 High (9.8) link
Summary:

PACKETSTORM:179290 High (8.1) link
Summary:

FB2E9ED1-43D7-585C-A197-0D6628B20134 High (8.1) link
Summary:

FA3992CE-9C4C-5350-8134-177126E0BD3F High (8.1) link
Summary:

F8981437-1287-5B69-93F1-657DFB1DCE59 High (8.1) link
Summary:

F58A5CB2-2174-586F-9CA9-4C47F8F38B5E High (8.1) link
Summary:

F1A00122-3797-11EF-B611-84A93843EB75 High (8.1) link
Summary:

EFD615F0-8F17-5471-AA83-0F491FD497AF High (8.1) link
Summary:

EC20B9C2-6857-5848-848A-A9F430D13EEB High (8.1) link
Summary:

EB13CBD6-BC93-5F14-A210-AC0B5A1D8572 High (8.1) link
Summary:

E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD High (8.1) link
Summary:

E543E274-C20A-582A-8F8E-F8E3F381C345 High (8.1) link
Summary:

E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257 High (8.1) link
Summary:

E24EEC0A-40F7-5BBC-9E4D-7B13522FF915 High (8.1) link
Summary:

DC798E98-BA77-5F86-9C16-0CF8CD540EBB High (8.1) link
Summary:

DC473885-F54C-5F76-BAFD-0175E4A90C1D High (8.1) link
Summary:

D85F08E9-DB96-55E9-8DD2-22F01980F360 High (8.1) link

Summary:

D572250A-BE94-501D-90C4-14A6C9C0AC47 High (8.1) link

Summary:

D1E049F1-393E-552D-80D1-675022B26911 High (8.1) link

Summary:

CVE-2024-6387 High (8.1) link

Summary:A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

CFEBF7AF-651A-5302-80B8-F8146D5B33A6 High (8.1) link

Summary:

CF80DDA9-42E7-5E06-8DA8-84C72658E191 High (8.1) link

Summary:

CB2926E1-2355-5C82-A42A-D4F72F114F9B High (8.1) link

Summary:

C6FB6D50-F71D-5870-B671-D6A09A95627F High (8.1) link

Summary:

C5B2D4A1-8C3B-5FF7-B620-EDE207B027A0 High (8.1) link

Summary:

C185263E-3E67-5550-B9C0-AB9C15351960 High (8.1) link

Summary:

BDA609DA-6936-50DC-A325-19FE2CC68562 High (8.1) link

Summary:

AA539633-36A9-53BC-97E8-19BC0E4E8D37 High (8.1) link

Summary:

A377249D-3C48-56C9-98D6-C47013B3A043 High (8.1) link

Summary:

9CDFE38D-80E9-55D4-A7A8-D5C20821303E High (8.1) link

Summary:

9A6454E9-662A-5A75-8261-73F46290FC3C High (8.1) link

Summary:

92254168-3B26-54C9-B9BE-B4B7563586B5 High (8.1) link

Summary:

91752937-D1C1-5913-A96F-72F8B8AB4280 High (8.1) link

Summary:

906CD901-3758-5F2C-8FA6-386BF9378AB3 High (8.1) link

Summary:

896B5857-A9C8-5342-934A-74F1EA1934CF High (8.1) link

Summary:

81F0C05A-8650-5DE8-97E9-0D89F1807E5D High (8.1) link
Summary:

7C7167AF-E780-5506-BEFA-02E5362E8E48 High (8.1) link
Summary:

7AA8980D-D89F-57EB-BFD1-18ED3AB1A7DD High (8.1) link
Summary:

79FE1ED7-EB3D-5978-A12E-AAB1FFECCCAC High (8.1) link
Summary:

795762E3-BAB4-54C6-B677-83B0ACC2B163 High (8.1) link
Summary:

77DAD6A9-8142-5591-8605-C5DADE4EE744 High (8.1) link
Summary:

743E5025-3BB8-5EC4-AC44-2AA679730661 High (8.1) link
Summary:

73A19EF9-346D-5B2B-9792-05D9FE3414E2 High (8.1) link
Summary:

6FD8F914-B663-533D-8866-23313FD37804 High (8.1) link
Summary:

6E81EAE5-2156-5ACB-9046-D792C7FAF698 High (8.1) link
Summary:

6B78D204-22B0-5D11-8A0C-6313958B473F High (8.1) link
Summary:

649197A2-0224-5B5C-9C4E-B5791D42A9FB High (8.1) link
Summary:

608FA50C-AEA1-5A83-8297-A15FC7D32A7C High (8.1) link
Summary:

5D2CB1F8-DC04-5545-8BC7-29EE3DA8890E High (8.1) link
Summary:

5C81C5C1-22D4-55B3-B843-5A9A60AAB6FD High (8.1) link
Summary:

58750D49-7302-11EF-8C95-195D300202B3 High (8.1) link
Summary:

56F97BB2-3DF6-5588-82AF-1D7B77F9AD45 High (8.1) link
Summary:

53BCD84F-BD22-5C9D-95B6-4B83627AB37F High (8.1) link
Summary:

535C5505-40BC-5D18-B346-1FDF036F0B08 High (8.1) link
Summary:

48603E8F-B170-57EE-85B9-67A7D9504891 High (8.1) link
Summary:

4748B283-C2F6-5924-8241-342F98EEC2EE High (8.1) link
Summary:

452ADB71-199C-561E-B949-FCDE6288B925 High (8.1) link
Summary:

418FD78F-82D2-5748-9EE9-CAFC34111864 High (8.1) link
Summary:

3D426DCE-96C7-5F01-B0AB-4B11C9557441 High (8.1) link
Summary:

31CC906F-9328-5944-B370-FBD98DF0DDD3 High (8.1) link
Summary:

2FFB4379-2BD1-569F-9F38-1B6D272234C9 High (8.1) link
Summary:

1FFDA397-F480-5C74-90F3-060E1FE11B2E High (8.1) link
Summary:

1F7A6000-9E6D-511C-B0F6-7CADB7200761 High (8.1) link
Summary:

1CF00BB8-B891-5347-A2DC-2C6A6BFF7C99 High (8.1) link
Summary:

1AB9F1F4-9798-59A0-9213-1D907E81E7F6 High (8.1) link
Summary:

1A779279-F527-5C29-A64D-94AAA4ADD6FD High (8.1) link
Summary:

15C36683-070A-5CC1-B21F-5F0BF974D9D3 High (8.1) link
Summary:

1337DAY-ID-39674 High (8.1) link
Summary:

123C2683-74BE-5320-AA3A-C376C8E3A992 High (8.1) link
Summary:

11F020AC-F907-5606-8805-0516E06160EE High (8.1) link
Summary:

108E1D25-1F7E-534C-97CD-3F6045E32B98 High (8.1) link
Summary:

0FC4BE81-312B-51F4-9D9B-66D8B5C093CD High (8.1) link
Summary:

0F9B3655-C7D4-55A9-8EB5-2EAD9CEAB180 High (8.1) link
Summary:

0E9294FD-6B44-503A-84C2-C6E76E53B0B7 High (8.1) link
Summary:

0A8CA57C-ED38-5301-A03A-C841BD3082EC High (8.1) link
Summary:

SSV:92579 High (7.5) link

Summary:

PACKETSTORM:173661 High (7.5) link

Summary:

F0979183-AE88-53B4-86CF-3AF0523F3807 High (7.5) link

Summary:

1337DAY-ID-26576 High (7.5) link

Summary:

CVE-2023-51385 Medium (6.5) link

Summary:In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

CVE-2023-48795 Medium (5.9) link

Summary:The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

CVE-2023-51384 Medium (5.5) link

Summary:In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

PACKETSTORM:140261 Low (0.0) link

Summary:

5C971D4B-2DD3-5894-9EC2-DAB952B4740D Low (0.0) link

Summary:

39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118 Low (0.0) link

Summary:

The above 95 vulnerabilities apply to these network locations:

- 192.168.2.2 Ports: ['22']
- 192.168.5.3 Ports: ['22']
- 192.168.1.2 Ports: ['22']

2 nginx 1.22.1 (cpe:/a:igor_sysoev:nginx:1.22.1)

DF1BBDC4-B715-5ABE-985E-91DD3BB87773 High (7.8) link
Summary:

676D4F16-4FB3-11ED-A374-8C164567CA3C High (7.8) link
Summary:

ADDC71B8-6024-11EF-86A1-8C164567CA3C Medium (5.7) link
Summary:

The above 3 vulnerabilities apply to these network locations:

- 192.168.5.3 Ports: ['80']
- 192.168.1.2 Ports: ['80']

3 PostgreSQL DB 15.5 - 15.6 (cpe:/a:postgresql:postgresql:15)

POSTGRESQL:CVE-2024-7348 High (8.8) link
Summary:

POSTGRESQL:CVE-2024-10979 High (8.8) link
Summary:

POSTGRESQL:CVE-2023-5869 High (8.8) link
Summary:

POSTGRESQL:CVE-2023-39417 High (8.8) link
Summary:

POSTGRESQL:CVE-2024-0985 High (8.0) link
Summary:

CVE-2022-2625 High (8.0) link

Summary:A vulnerability was found in PostgreSQL. This attack requires permission to create non-temporary objects in at least one schema, the ability to lure or wait for an administrator to create or update an affected extension in that schema, and the ability to lure or wait for a victim to use the object targeted in CREATE OR REPLACE or CREATE IF NOT EXISTS. Given all three prerequisites, this flaw allows an attacker to run arbitrary code as the victim role, which may be a superuser.

POSTGRESQL:CVE-2023-2455 High (7.5) link

Summary:

POSTGRESQL:CVE-2023-2454 High (7.2) link

Summary:

CVE-2023-2454 High (7.2) link

Summary:schema_element defeats protective search_path changes; It was found that certain database calls in PostgreSQL could permit an authed attacker with elevated database-level privileges to execute arbitrary code.

CVE-2023-2455 Medium (5.4) link

Summary:Row security policies disregard user ID changes after inlining; PostgreSQL could permit incorrect policies to be applied in certain cases where role-specific policies are used and a given query is planned under one role and then executed under other roles. This scenario can happen under security definer functions or when a common user and query is planned initially and then re-used across multiple SET ROLEs. Applying an incorrect policy may permit a user to complete otherwise-forbidden reads and modifications. This affects only databases that have used CREATE POLICY to define a row security policy.

POSTGRESQL:CVE-2023-5870 Medium (4.4) link

Summary:

POSTGRESQL:CVE-2023-5868 Medium (4.3) link

Summary:

POSTGRESQL:CVE-2023-39418 Medium (4.3) link

Summary:

POSTGRESQL:CVE-2024-10978 Medium (4.2) link

Summary:

POSTGRESQL:CVE-2024-10976 Medium (4.2) link

Summary:

POSTGRESQL:CVE-2022-41862 Low (3.7) link

Summary:

POSTGRESQL:CVE-2024-4317 Low (3.1) link

Summary:

POSTGRESQL:CVE-2024-10977 Low (3.1) link

Summary:

The above 18 vulnerabilities apply to these network locations:

- 192.168.3.2 Ports: ['5432']

List of IPs Scanned

- 192.168.1.0/30
- 192.168.2.0/30
- 192.168.3.0/30
- 192.168.4.0/30
- 192.168.5.0/30