Openssh: machine-in-the-middle attack if verifyhostkeydns is enabled

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-26465
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-18 19:15:29 UTC
Updated	2026-05-12 13:16:40 UTC
Description	A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can

Risk And Classification

Primary CVSS: v3.1 6.8 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

Problem Types: CWE-390 | CWE-390 Detection of Error Condition Without Action

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N
3.1	secalert@redhat.com	Secondary	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

vailability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	12.0	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Ontap	9	All	All	All
Application	Openbsd	Openssh	6.8	p1	All	All
Application	Openbsd	Openssh	9.9	-	All	All
Application	Openbsd	Openssh	9.9	p1	All	All
Application	Openbsd	Openssh	All	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:8.0p1-26.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:8.0p1-26.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:8.7p1-45.el9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:8.7p1-45.el9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:8.7p1-38.el9_4.5 * rpm
CNA	Red Hat	Red Hat Discovery 1.14	unaffected sha256:f33991d766b618a128fb99fbe4f9b61c5004
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom

References

Reference	Source	Link
www.openwall.com/lists/oss-security/2025/02/18/1	af854a3a-2127-422b-91ae-364da2661108	www.openwall
www.theregister.com/2025/02/18/openssh_vulnerabilities_mitm_dos	af854a3a-2127-422b-91ae-364da2661108	www.theregist
bugzilla.suse.com/show_bug.cgi	af854a3a-2127-422b-91ae-364da2661108	bugzilla.suse.c
ubuntu.com/security/CVE-2025-26465	af854a3a-2127-422b-91ae-364da2661108	ubuntu.com
seclists.org/fulldisclosure/2025/May/7	af854a3a-2127-422b-91ae-364da2661108	seclists.org
ftp.openbsd.org/pub/OpenBSD/patches/7.6/common/008_ssh.patch.sig	af854a3a-2127-422b-91ae-364da2661108	ftp.openbsd.or
access.redhat.com/security/cve/CVE-2025-26465	secalert@redhat.com	access.redhat.
access.redhat.com/errata/RHSA-2025:6993	secalert@redhat.com	access.redhat.
www.vicarius.io/vsociety/posts/cve-2025-26465-mitigate-vulnerable-openssh	af854a3a-2127-422b-91ae-364da2661108	www.vicarius.i
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.sier
access.redhat.com/solutions/7109879	secalert@redhat.com	access.redhat.
security.netapp.com/advisory/ntap-20250228-0003	af854a3a-2127-422b-91ae-364da2661108	security.netapp
blog.qualys.com/vulnerabilities-threat-research/2025/02/18/qualys-tru-discove...	af854a3a-2127-422b-91ae-364da2661108	blog.qualys.co
www.openwall.com/lists/oss-security/2025/02/18/4	af854a3a-2127-422b-91ae-364da2661108	www.openwall
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat
lists.debian.org/debian-lts-announce/2025/02/msg00020.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
www.vicarius.io/vsociety/posts/cve-2025-26465-detect-vulnerable-openssh	af854a3a-2127-422b-91ae-364da2661108	www.vicarius.i
seclists.org/fulldisclosure/2025/May/8	af854a3a-2127-422b-91ae-364da2661108	seclists.org
www.openssh.com/releasenotes.html	af854a3a-2127-422b-91ae-364da2661108	www.openssh.
lists.mindrot.org/pipermail/openssh-unix-announce/2025-February/000161.html	af854a3a-2127-422b-91ae-364da2661108	lists.mindrot.or
security-tracker.debian.org/tracker/CVE-2025-26465	af854a3a-2127-422b-91ae-364da2661108	security-tracke
access.redhat.com/errata/RHSA-2025:3837	secalert@redhat.com	access.redhat.
access.redhat.com/errata/RHSA-2025:16823	secalert@redhat.com	access.redhat.
seclists.org/fulldisclosure/2025/Feb/18	af854a3a-2127-422b-91ae-364da2661108	seclists.org
access.redhat.com/errata/RHSA-2025:8385	secalert@redhat.com	access.redhat.
seclists.org/oss-sec/2025/q1/144	134c704f-9b21-4f2e-91b3-4a467353bcc0	seclists.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event

Source	Time	Event
CNA	2025-02-10T21:56:03.853Z	Reported to Red Hat.
CNA	2025-02-17T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

There are currently no legacy QID mappings associated with this CVE.