Openssh: regresshion - race condition in ssh allows rce/dos

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

Summary

CVE	CVE-2024-6387
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-01 13:15:06 UTC
Updated	2026-05-12 12:17:20 UTC
Description	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can le

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from nvd@nist.gov

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

Problem Types: CWE-364 | CWE-362 | CWE-364 Signal Handler Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	secalert@redhat.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

vailability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Almalinux	Almalinux	9.0	-	All	All
Operating System	Apple	Macos	All	All	All	All
Operating System	Arista	Eos	All	All	All	All
Operating System	Canonical	Ubuntu Linux	23.10	All	All	All
Operating System	Canonical	Ubuntu Linux	24.04	All	All	All
Hardware	Netapp	500f	-	All	All	All
Operating System	Netapp	500f Firmware	-	All	All	All
Hardware	Netapp	8300	-	All	All	All
Operating System	Netapp	8300 Firmware	-	All	All	All
Hardware	Netapp	8700	-	All	All	All
Operating System	Netapp	8700 Firmware	-	All	All	All
Hardware	Netapp	A150	-	All	All	All
Operating System	Netapp	A150 Firmware	-	All	All	All
Hardware	Netapp	A1k	-	All	All	All
Operating System	Netapp	A1k Firmware	-	All	All	All
Hardware	Netapp	A220	-	All	All	All
Operating System	Netapp	A220 Firmware	-	All	All	All
Hardware	Netapp	A250	-	All	All	All
Operating System	Netapp	A250 Firmware	-	All	All	All
Hardware	Netapp	A400	-	All	All	All
Operating System	Netapp	A400 Firmware	-	All	All	All
Hardware	Netapp	A70	-	All	All	All
Hardware	Netapp	A700s	-	All	All	All
Operating System	Netapp	A700s Firmware	-	All	All	All
Operating System	Netapp	A70 Firmware	-	All	All	All
Hardware	Netapp	A800	-	All	All	All
Operating System	Netapp	A800 Firmware	-	All	All	All
Hardware	Netapp	A90	-	All	All	All

Hardware	Netapp	A900	-	All	All	All
Operating System	Netapp	A900 Firmware	-	All	All	All
Operating System	Netapp	A90 Firmware	-	All	All	All
Hardware	Netapp	A9500	-	All	All	All
Operating System	Netapp	A9500 Firmware	-	All	All	All
Operating System	Netapp	Bootstrap Os	-	All	All	All
Hardware	Netapp	C190	-	All	All	All
Operating System	Netapp	C190 Firmware	-	All	All	All
Hardware	Netapp	C250	-	All	All	All
Operating System	Netapp	C250 Firmware	-	All	All	All
Hardware	Netapp	C400	-	All	All	All
Operating System	Netapp	C400 Firmware	-	All	All	All
Hardware	Netapp	C800	-	All	All	All
Operating System	Netapp	C800 Firmware	-	All	All	All
Hardware	Netapp	Fas2720	-	All	All	All
Operating System	Netapp	Fas2720 Firmware	-	All	All	All
Hardware	Netapp	Fas2750	-	All	All	All
Operating System	Netapp	Fas2750 Firmware	-	All	All	All
Hardware	Netapp	Fas2820	-	All	All	All
Operating System	Netapp	Fas2820 Firmware	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Hardware	Sonicwall	Sma 6200	-	All	All	All
Operating System	Sonicwall	Sma 6200 Firmware	-	All	All	All
Hardware	Sonicwall	Sma 6210	-	All	All	All
Operating System	Sonicwall	Sma 6210 Firmware	-	All	All	All
Hardware	Sonicwall	Sma 7200	-	All	All	All
Operating System	Sonicwall	Sma 7200 Firmware	-	All	All	All
Hardware	Sonicwall	Sma 7210	-	All	All	All
Operating System	Sonicwall	Sma 7210 Firmware	-	All	All	All
Hardware	Sonicwall	Sma 8200v	-	All	All	All
Operating System	Sonicwall	Sma 8200v Firmware	-	All	All	All
Hardware	Sonicwall	Sra Ex 7000	-	All	All	All
Operating System	Sonicwall	Sra Ex 7000 Firmware	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platfor

CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:8.7p1-38.el9_4.1 * rpm	Not spe
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:8.7p1-38.el9_4.1 * rpm	Not spe
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:8.7p1-12.el9_0.1 * rpm	Not spe
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Extended Update Support	unaffected 0:8.7p1-30.el9_2.4 * rpm	Not spe
CNA	Red Hat	Red Hat OpenShift Container Platform 4.13	unaffected 413.92.202407091321-0 * rpm	Not spe
CNA	Red Hat	Red Hat OpenShift Container Platform 4.14	unaffected 414.92.202407091253-0 * rpm	Not spe
CNA	Red Hat	Red Hat OpenShift Container Platform 4.15	unaffected 415.92.202407091355-0 * rpm	Not spe
CNA	Red Hat	Red Hat OpenShift Container Platform 4.16	unaffected 416.94.202407081958-0 * rpm	Not spe
CNA	Red Hat	Red Hat Ceph Storage 5	Not specified	Not spe
CNA	Red Hat	Red Hat Ceph Storage 6	Not specified	Not spe
CNA	Red Hat	Red Hat Ceph Storage 7	Not specified	Not spe
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not spe
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not spe
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not spe
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not spe
ADP	Siemens	Industrial Edge Management OS IEM-OS	affected * custom	Not spe
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not spe
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not spe
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not spe
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not spe
ADP	Siemens	SINAMICS IIoT Module	affected V1.0 HF1 custom	Not spe
ADP	Siemens	SINEMA Remote Connect Server	affected V3.2 SP2 custom	Not spe
ADP	Siemens	SINUMERIK ONE	affected V6.24 custom	Not spe
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not spe

References

Reference	Source	Link
www.openwall.com/lists/oss-security/2024/07/03/1	af854a3a-2127-422b-91ae-364da2661108	www.o
www.openwall.com/lists/oss-security/2024/07/10/6	af854a3a-2127-422b-91ae-364da2661108	www.o
www.exploit-db.com/exploits/52269	af854a3a-2127-422b-91ae-364da2661108	www.e
github.com/zgzhang/cve-2024-6387-poc	af854a3a-2127-422b-91ae-364da2661108	github.
www.openwall.com/lists/oss-security/2024/07/09/2	af854a3a-2127-422b-91ae-364da2661108	www.o
ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2024-002.txt.asc	af854a3a-2127-422b-91ae-364da2661108	ftp.netb
www.openwall.com/lists/oss-security/2024/07/23/4	af854a3a-2127-422b-91ae-364da2661108	www.o
github.com/Azure/AKS/issues/4379	af854a3a-2127-422b-91ae-364da2661108	github.

bugzilla.redhat.com/show_bug.cgi	af854a3a-2127-422b-91ae-364da2661108	bugzill
www.arista.com/en/support/advisories-notices/security-advisory/19904-securit...	af854a3a-2127-422b-91ae-364da2661108	www.a
github.com/PowerShell/Win32-OpenSSH/issues/2249	af854a3a-2127-422b-91ae-364da2661108	github.
www.vicarius.io/vsociety/posts/regresshion-an-openssh-regression-error-cve-20...	af854a3a-2127-422b-91ae-364da2661108	www.v
www.openwall.com/lists/oss-security/2024/07/03/3	af854a3a-2127-422b-91ae-364da2661108	www.o
www.openwall.com/lists/oss-security/2024/07/10/4	af854a3a-2127-422b-91ae-364da2661108	www.o
lists.almalinux.org/archives/list/announce@lists.almalinux.org/thread/23BF5BMGFVE...	af854a3a-2127-422b-91ae-364da2661108	lists.al
www.openwall.com/lists/oss-security/2024/07/03/2	af854a3a-2127-422b-91ae-364da2661108	www.o
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-po
santandersecurityresearch.github.io/blog/sshing_the_masses.html	af854a3a-2127-422b-91ae-364da2661108	santan
github.com/oracle/oracle-linux/issues/149	af854a3a-2127-422b-91ae-364da2661108	github.
access.redhat.com/errata/RHSA-2024:4389	af854a3a-2127-422b-91ae-364da2661108	access
www.openwall.com/lists/oss-security/2024/07/23/6	af854a3a-2127-422b-91ae-364da2661108	www.o
ubuntu.com/security/CVE-2024-6387	af854a3a-2127-422b-91ae-364da2661108	ubuntu
support.apple.com/kb/HT214120	af854a3a-2127-422b-91ae-364da2661108	suppor
www.openwall.com/lists/oss-security/2024/07/10/2	af854a3a-2127-422b-91ae-364da2661108	www.o
www.openwall.com/lists/oss-security/2024/07/04/2	af854a3a-2127-422b-91ae-364da2661108	www.o
psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0010	af854a3a-2127-422b-91ae-364da2661108	psirt.gl
access.redhat.com/security/cve/CVE-2024-6387	af854a3a-2127-422b-91ae-364da2661108	access
www.openwall.com/lists/oss-security/2024/07/03/5	af854a3a-2127-422b-91ae-364da2661108	www.o
news.ycombinator.com/item	af854a3a-2127-422b-91ae-364da2661108	news.y
security.netapp.com/advisory/ntap-20240701-0001	af854a3a-2127-422b-91ae-364da2661108	securit
support.apple.com/kb/HT214118	af854a3a-2127-422b-91ae-364da2661108	suppor
www.openwall.com/lists/oss-security/2024/07/10/3	af854a3a-2127-422b-91ae-364da2661108	www.o
www.openwall.com/lists/oss-security/2024/07/03/4	af854a3a-2127-422b-91ae-364da2661108	www.o
access.redhat.com/errata/RHSA-2024:4479	af854a3a-2127-422b-91ae-364da2661108	access
github.com/openela-main/openssh/commit/e1f438970e5a337a17070a637c1b9e196...	af854a3a-2127-422b-91ae-364da2661108	github.
blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote...	af854a3a-2127-422b-91ae-364da2661108	blog.qu
www.akamai.com/blog/security-research/2024-openssh-vulnerability-regression-...	af854a3a-2127-422b-91ae-364da2661108	www.a
lists.mindrot.org/pipermail/openssh-unix-announce/2024-July/000158.html	af854a3a-2127-422b-91ae-364da2661108	lists.mi
www.openwall.com/lists/oss-security/2024/07/09/5	af854a3a-2127-422b-91ae-364da2661108	www.o
www.openwall.com/lists/oss-security/2024/07/10/1	af854a3a-2127-422b-91ae-364da2661108	www.o
www.openwall.com/lists/oss-security/2024/07/04/1	af854a3a-2127-422b-91ae-364da2661108	www.o
www.theregister.com/2024/07/01/regresshion_openssh	af854a3a-2127-422b-91ae-364da2661108	www.th
sig-security.rocky.page/issues/CVE-2024-6387	af854a3a-2127-422b-91ae-364da2661108	sig-sec

security-tracker.debian.org/tracker/CVE-2024-6387	af854a3a-2127-422b-91ae-364da2661108	securit
www.freebsd.org/security/advisories/FreeBSD-SA-24:04.openssh.asc	af854a3a-2127-422b-91ae-364da2661108	www.fr
www.splunk.com/en_us/blog/security/cve-2024-6387-regresshion-vulnerability.html	af854a3a-2127-422b-91ae-364da2661108	www.s
www.openwall.com/lists/oss-security/2024/07/28/2	af854a3a-2127-422b-91ae-364da2661108	www.o
www.openwall.com/lists/oss-security/2024/07/11/3	af854a3a-2127-422b-91ae-364da2661108	www.o
github.com/microsoft/azurelinux/issues/9555	af854a3a-2127-422b-91ae-364da2661108	github.
stackdiary.com/openssh-race-condition-in-sshd-allows-remote-code-execution	af854a3a-2127-422b-91ae-364da2661108	stackdi
www.openwall.com/lists/oss-security/2024/07/28/3	af854a3a-2127-422b-91ae-364da2661108	www.o
packetstorm.news/files/id/190587	af854a3a-2127-422b-91ae-364da2661108	packet
seclists.org/fulldisclosure/2024/Jul/20	af854a3a-2127-422b-91ae-364da2661108	seclists
arstechnica.com/security/2024/07/regresshion-vulnerability-in-openssh-gives-a...	af854a3a-2127-422b-91ae-364da2661108	arstech
cert-portal.siemens.com/productcert/html/ssa-446545.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-po
www.openwall.com/lists/oss-security/2024/07/01/12	af854a3a-2127-422b-91ae-364da2661108	www.o
seclists.org/fulldisclosure/2024/Jul/18	af854a3a-2127-422b-91ae-364da2661108	seclists
access.redhat.com/errata/RHSA-2024:4484	af854a3a-2127-422b-91ae-364da2661108	access
www.openwall.com/lists/oss-security/2024/07/11/1	af854a3a-2127-422b-91ae-364da2661108	www.o
support.apple.com/kb/HT214119	af854a3a-2127-422b-91ae-364da2661108	suppor
access.redhat.com/errata/RHSA-2024:4474	af854a3a-2127-422b-91ae-364da2661108	access
www.openwall.com/lists/oss-security/2024/07/01/13	af854a3a-2127-422b-91ae-364da2661108	www.o
forum.vmssoftware.com/viewtopic.php	af854a3a-2127-422b-91ae-364da2661108	forum.v
access.redhat.com/errata/RHSA-2024:4312	af854a3a-2127-422b-91ae-364da2661108	access
www.openwall.com/lists/oss-security/2024/07/08/2	af854a3a-2127-422b-91ae-364da2661108	www.o
www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt	af854a3a-2127-422b-91ae-364da2661108	www.q
access.redhat.com/errata/RHSA-2024:4340	af854a3a-2127-422b-91ae-364da2661108	access
seclists.org/fulldisclosure/2024/Jul/19	af854a3a-2127-422b-91ae-364da2661108	seclists
github.com/PowerShell/Win32-OpenSSH/discussions/2248	af854a3a-2127-422b-91ae-364da2661108	github.
www.suse.com/security/cve/CVE-2024-6387.html	af854a3a-2127-422b-91ae-364da2661108	www.s
www.openwall.com/lists/oss-security/2024/07/08/3	af854a3a-2127-422b-91ae-364da2661108	www.o
www.openwall.com/lists/oss-security/2024/07/02/1	af854a3a-2127-422b-91ae-364da2661108	www.o
github.com/AlmaLinux/updates/issues/629	af854a3a-2127-422b-91ae-364da2661108	github.
lists.mindrot.org/pipermail/openssh-unix-dev/2024-July/041431.html	af854a3a-2127-422b-91ae-364da2661108	lists.mi
www.openssh.com/txt/release-9.8	af854a3a-2127-422b-91ae-364da2661108	www.o
archlinux.org/news/the-sshd-service-needs-to-be-restarted-after-upgrading-t...	af854a3a-2127-422b-91ae-364da2661108	archlin
www.openwall.com/lists/oss-security/2024/07/03/11	af854a3a-2127-422b-91ae-364da2661108	www.o
access.redhat.com/errata/RHSA-2024:4469	af854a3a-2127-422b-91ae-364da2661108	access
explore.alas.aws.amazon.com/CVE-2024-6387.html	af854a3a-2127-422b-91ae-364da2661108	explore

ubuntu.com/security/notices/USN-6859-1	af854a3a-2127-422b-91ae-364da2661108	ubuntu
github.com/rapier1/hpn-ssh/issues/87	af854a3a-2127-422b-91ae-364da2661108	github.
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Qualys Threat Research Unit (TRU) (Qualys) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-06-27T00:00:00.000Z	Reported to Red Hat.
CNA	2024-07-01T08:00:00.000Z	Made public.

Workarounds

CNA: The below process can protect against a Remote Code Execution attack by disabling the LoginGraceTime parameter on Red Hat Enterprise Linux 9. However, the sshd server is still vulnerable to a Denial of Service if an attacker exhausts all the connections. 1) As root user, open the /etc/ssh/sshd_config 2) Add or edit the parameter configuration: ~~~ LoginGraceTime 0 ~~~ 3) Save and close the file 4) Restart the sshd daemon: ~~~ systemctl restart sshd.service ~~~ Setting LoginGraceTime to 0 disables the SSHD server's ability to drop connections if authentication is not completed within the specified timeout. If this mitigation is implemented, it is highly recommended to use a tool like 'fail2ban' alongside a firewall to monitor log files and manage connections appropriately. If any of the mitigations mentioned above is used, please note that the removal of LoginGraceTime parameter from sshd_config is not automatic when the updated package is installed.

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