



CVE-2023-38408

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-38408
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-20 03:15:00 UTC
Updated	2023-11-07 04:17:00 UTC
Description	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remo

Risk And Classification

Problem Types: CWE-428

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Openbsd	Openssh	9.3	-	All	All
Application	Openbsd	Openssh	9.3	p1	All	All

References

Reference	Source	Link
[SECURITY] Fedora 38 Update: openssh-9.0p1-16.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
oss-security - Re: Announce: OpenSSH 9.3p2 released	MLIST	www.openwall.com
CVE-2023-38408: Remote Code Execution in OpenSSH's forwarded ssh-agent Qualys Security Blog	MISC	blog.qualys.com
oss-security - Re: illumos (or at least danmcd) membership in the distros list	MLIST	www.openwall.com
[SECURITY] [DLA 3532-1] openssh security update	MLIST	lists.debian.org
www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt	MISC	www.qualys.com
CVE-2023-38408 OpenSSH Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 37 Update: openssh-8.8p1-11.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 37 Update: openssh-8.8p1-11.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org

oss-security - Re: CVE-2023-38408: Remote Code Execution in OpenSSH's forwarded ssh-agent	MLIST	www.openwall.com
OpenSSH Forwarded SSH-Agent Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com
Disallow remote addition of FIDO/PKCS11 provider libraries to · openbsd/src@7bc29a9 · GitHub	MISC	github.com
terminate process if requested to load a PKCS#11 provider that · openbsd/src@f03a4fa · GitHub	MISC	github.com
oss-security - Re: illumos (or at least danmcd) membership in the distros list	MLIST	www.openwall.com
OpenSSH: Security	CONFIRM	www.openssh.com
[SECURITY] Fedora 38 Update: openssh-9.0p1-16.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Ensure FIDO/PKCS11 libraries contain expected symbols · openbsd/src@f8f5a6b · GitHub	MISC	github.com
Remote code execution in OpenSSH's forwarded SSH-agent Hacker News	MISC	news.ycombinator.com
OpenSSH: Remote Code Execution (GLSA 202307-01) — Gentoo security	GENTOO	security.gentoo.org
www.openssh.com/txt/release-9.3p2	CONFIRM	www.openssh.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [160826](#) Oracle Enterprise Linux Security Update for openssh (ELSA-2023-4412)
- [160828](#) Oracle Enterprise Linux Security Update for openssh (ELSA-2023-4419)
- [160836](#) Oracle Enterprise Linux Security Update for openssh (ELSA-2023-4382)
- [160862](#) Oracle Enterprise Linux Security Update for openssh (ELSA-2023-12711)
- [160867](#) Oracle Enterprise Linux Security Update for openssh (ELSA-2023-4428)
- [199596](#) Ubuntu Security Notification for OpenSSH Vulnerability (USN-6242-1)
- [199628](#) Ubuntu Security Notification for OpenSSH Vulnerability (USN-6242-2)
- [241870](#) Red Hat Update for openssh (RHSA-2023:4329)
- [241877](#) Red Hat Update for openssh (RHSA-2023:4382)
- [241879](#) Red Hat Update for openssh (RHSA-2023:4381)
- [241882](#) Red Hat Update for openssh (RHSA-2023:4383)
- [241885](#) Red Hat Update for openssh (RHSA-2023:4384)
- [241896](#) Red Hat Update for openssh (RHSA-2023:4419)
- [241897](#) Red Hat Update for openssh (RHSA-2023:4413)
- [241899](#) Red Hat Update for openssh (RHSA-2023:4412)

257251 CentOS Security Update for openssh
257283 CentOS Security Update for openssh (CESA-2023:4382)
284332 Fedora Security Update for openssh (FEDORA-2023-878e04f4ae)
284355 Fedora Security Update for openssh (FEDORA-2023-79a18e1725)
296108 Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
355783 Amazon Linux Security Advisory for openssh : ALAS2-2023-2176
355801 Amazon Linux Security Advisory for openssh : ALAS2023-2023-273
355819 Amazon Linux Security Advisory for openssh : ALAS-2023-1802
378752 Alibaba Cloud Linux Security Update for openssh (ALINUX3-SA-2023:0090)
378760 Alibaba Cloud Linux Security Update for openssh (ALINUX2-SA-2023:0033)
38904 OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent
390278 Oracle Managed Virtualization (VM) Server for x86 Security Update for openssh (OVMSA-2023-0019)
503049 Alpine Linux Security Update for openssh
503052 Alpine Linux Security Update for openssh
6000161 Debian Security Update for openssh (DLA 3532-1)
673431 EulerOS Security Update for openssh (EulerOS-SA-2023-2792)
673531 EulerOS Security Update for openssh (EulerOS-SA-2023-2816)
673546 EulerOS Security Update for openssh (EulerOS-SA-2023-2882)
673578 EulerOS Security Update for openssh (EulerOS-SA-2023-2846)
673903 EulerOS Security Update for openssh (EulerOS-SA-2023-2863)
674038 EulerOS Security Update for openssh (EulerOS-SA-2023-3140)
674099 EulerOS Security Update for openssh (EulerOS-SA-2023-2901)
691219 Free Berkeley Software Distribution (FreeBSD) Security Update for openssh (887eb570-27d3-11ee-adba-c80aa9043978)
710742 Gentoo Linux OpenSSH Remote Code Execution (RCE) Vulnerability (GLSA 202307-01)
754200 SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2023:2950-1)
754201 SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2023:2947-1)
754202 SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2023:2946-1)
754203 SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2023:2945-1)

907113 Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (27625-1)

907218 Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (27651-1)

941195 AlmaLinux Security Update for openssh (ALSA-2023:4419)

941196 AlmaLinux Security Update for openssh (ALSA-2023:4412)

960973 Rocky Linux Security Update for openssh (RLSA-2023:4419)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)