CVE-2020-8794

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

Summary

CVE	CVE-2020-8794
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-25 17:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	OpenSMTPD before 6.6.4 allows remote code execution because of an out-of-bounds read in mta_io in mta_session.c for r

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Opensmtpd	Opensmtpd	All	All	All	All
Application	Opensmtpd	Opensmtpd	All	All	All	All

References

Reference	Source	Link
oss-security - Re: LPE and RCE in OpenSMTPD's default install (CVE-2020-8794)	MLIST	www.openwall.com
oss-security - 21Nails: Multiple vulnerabilities in Exim	MLIST	www.openwall.com
Debian -- Security Information -- DSA-4634-1 opensmtpd	DEBIAN	www.debian.org
USN-4294-1: OpenSMTPD vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com
OpenSMTPD Out-Of-Bounds Read / Local Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.co
oss-security - Re: LPE and RCE in OpenSMTPD's default install (CVE-2020-8794)	MLIST	www.openwall.com

[SECURITY] Fedora 32 Update: opensmtpd-6.6.4p1-2.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 32 Update: opensmtpd-6.6.4p1-2.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Full Disclosure: LPE and RCE in OpenSMTPD's default install (CVE-2020-8794)	FULLDISC	seclists.org
oss-security - Re: LPE and RCE in OpenSMTPD's default install (CVE-2020-8794)	MLIST	www.openwall.com
OpenBSD Security	MISC	www.openbsd.org
oss-security - LPE and RCE in OpenSMTPD's default install (CVE-2020-8794)	MISC	www.openwall.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

501653 Alpine Linux Security Update for opensmtpd-extras

505194 Alpine Linux Security Update for opensmtpd-extras

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**