



# CVE-2020-8794

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

## Summary

<b>CVE</b>	CVE-2020-8794
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-02-25 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">Opensmtpd</a>	<a href="#">Opensmtpd</a>	All	All	All	All
Application	<a href="#">Opensmtpd</a>	<a href="#">Opensmtpd</a>	All	All	All	All

## References

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

[SECURITY] Fedora 32 Update: openssl-1.1.1-2.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 32 Update: openssl-1.1.1-2.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Full Disclosure: LPE and RCE in OpenSMTPD's default install (CVE-2020-8794)	FULLDISC	<a href="https://seclists.org">seclists.org</a>
oss-security - Re: LPE and RCE in OpenSMTPD's default install (CVE-2020-8794)	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
OpenBSD Security	MISC	<a href="https://www.openbsd.org">www.openbsd.org</a>
oss-security - LPE and RCE in OpenSMTPD's default install (CVE-2020-8794)	MISC	<a href="https://www.openwall.com">www.openwall.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[501653](#) Alpine Linux Security Update for openssl-1.1.1-2.fc32

[505194](#) Alpine Linux Security Update for openssl-1.1.1-2.fc32

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)