



CVE-2020-7247

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

Summary

CVE	CVE-2020-7247
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-29 16:15:00 UTC
Updated	2023-11-07 03:25:00 UTC
Description	smtp_mailaddr in smtp_session.c in OpenSMTPD 6.6, as used in OpenBSD 6.6 and other products, allows remote attacker

Risk And Classification

EPSS: 0.940760000 probability, percentile 0.999030000 (date 2026-04-01)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-78 | CWE-755

CISA Known Exploited Vulnerability

Vendor	OpenBSD
Product	OpenSMTPD
Name	OpenSMTPD Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-7247

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	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Openbsd	Opensmtpd	6.6	All	All	All

Application	Openbsd	Opensmtpd	6.6	All	All	All
-------------	---------	-----------	-----	-----	-----	-----

References			
Reference	Source	Link	
Debian -- Security Information -- DSA-4611-1 opensmtpd	DEBIAN	www.debian.org	
Full Disclosure: LPE and RCE in OpenSMTPD (CVE-2020-7247)	FULLDISC	seclists.org	
OpenSMTPD 6.6.1 Local Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	
[SECURITY] Fedora 32 Update: opensmtpd-6.6.4p1-2.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
USN-4268-1: OpenSMTPD vulnerability Ubuntu security notices	UBUNTU	usn.ubuntu.com	
[SECURITY] Fedora 32 Update: opensmtpd-6.6.4p1-2.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
OpenSMTPD 6.6.2 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
OpenSMTPD MAIL FROM Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
OpenBSD OpenSMTPD Privilege Escalation / Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
oss-security - LPE and RCE in OpenSMTPD (CVE-2020-7247)	MISC	www.openwall.com	
OpenBSD OpenSMTPD 6.6 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
VU#390745 - OpenSMTPD vulnerable to local privilege escalation and remote code execution	CERT-VN	www.kb.cert.org	
OpenBSD Security	CONFIRM	www.openbsd.org	
Bugtraq: [SECURITY] [DSA 4611-1] opensmtpd security update	BUGTRAQ	seclists.org	
Fix a security vulnerability discovered by Qualys which can lead to a · openbsd/src@9dcfda0 · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	
NVD vulnerability detail	NVD	nvd.nist.gov	
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500482](#) Alpine Linux Security Update for opensmtpd

[505195](#) Alpine Linux Security Update for opensmtpd

© [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](#).

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