

CVE-2020-7247

OpenBSD OpenSMTPD Remote Code Execution Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

smtp_mailaddr in smtp_session.c in OpenSMTPD 6.6, as used in OpenBSD 6.6 and other products, allows remote attackers to execute arbitrary commands as root via a crafted SMTP session, as demonstrated by shell metacharacters in a MAIL FROM field. This affects the "uncommented" default configuration. The issue exists because of an incorrect return value upon failure of input validation.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.990 99.93rd percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.990 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified
CISA required action: Apply updates per vendor instructions.
 Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
opensmtpd	6.6	no fixed version listed	NVD
debian linux	9.0 10.0	no fixed version listed	NVD
fedora	32	no fixed version listed	NVD
ubuntu linux	18.04 19.10	no fixed version listed	NVD

Sources

Vendor guidance github.com/openbsd/src/commit/9dcfda045474d8903224d175907bfc29761dcb45
NVD nvd.nist.gov/vuln/detail/CVE-2020-7247

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-28374

Additional guidance openbsd.org/security.html

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2020-7247

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.