

CVE-2018-6789

Exim Buffer Overflow Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

An issue was discovered in the base64d function in the SMTP listener in Exim before 4.90.1. By sending a handcrafted message, a buffer overflow may happen. This can be used to execute code remotely.

EVRS 89 / ₁₀₀ Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.821 99.66th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.821 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
exim	< 4.90.1	4.90.1	NVD
debian linux	7.0 8.0 9.0	no fixed version listed	NVD
ubuntu linux	14.04 16.04 17.10	no fixed version listed	NVD

Sources

Vendor guidance	git.exim.org/exim.git/commit/cf3cd306062a08969c41a1cdd32c6855f1abecf1	NVD	nvd.nist.gov/vuln/detail/CVE-2018-6789
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2018-18536
Current data	evulnable.com/vulnerability-management/cve/CVE-2018-6789		

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