

CVE-2025-32433

Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability

Exigent

CISA KEV since Jun 9, 2025

Actively exploited

Public exploit module (Metasploit)

Erlang/OTP is a set of libraries for the Erlang programming language. Prior to versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20, a SSH server may allow an attacker to perform unauthenticated remote code execution (RCE). By exploiting a flaw in SSH protocol message handling, a malicious actor could gain unauthorized access to affected systems and execute arbitrary commands without valid credentials. This issue is patched in versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. A temporary workaround involves disabling the SSH server or to prevent access via firewall rules.

EVRS

88/100

Immediate priority

CVSS V3.1

10.0

Critical · NVD

EPSS

0.988

99.93rd percentile · FIRST

CISA DEADLINE

Jun 30, 2025

KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.988 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source project, third-party library, or a protocol used by different products.

Basis: CISA KEV required action

Affected and fixed versions · 28 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
erlang\otp	< 25.3.2.20 ≥ 26.0 < 26.2.5.11 ≥ 27.0 < 27.3.3	no fixed version listed	NVD
confd basic	< 7.7.19.1 ≥ 8.0.18 < 8.1.16.2 ≥ 8.2 < 8.2.11.1 ≥ 8.3 < 8.3.8.1 ≥ 8.4 < 8.4.4.1	no fixed version listed	NVD
network services orchestrator	< 5.7.19.1 ≥ 5.8 < 6.1.16.2 ≥ 6.2 < 6.2.11.1 ≥ 6.3 < 6.3.8.1 ≥ 6.4 < 6.4.1.1 ≥ 6.4.2 < 6.4.4.1	no fixed version listed	NVD
cloud native broadband network gateway	< 2025.03.1	no fixed version listed	NVD



PACKAGE	AFFECTED	FIXED IN	SOURCE
inode manager	–	no fixed version listed	NVD
smart phy	< 25.2	no fixed version listed	NVD
ultra packet core	< 2025.03	no fixed version listed	NVD
ultra services platform	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/erlang/otp/commit/0fcd9c56524b28615e8ece65fc0c3f66ef6e4c12	Additional guidance	github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2
sec.cloudapps.cisco.com	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-erlang-otp-ssh-xyZZy	NVD	nvd.nist.gov/vuln/detail/CVE-2025-32433
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-11793
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-32433		

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