مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Vulnerability in Erlang/OTP

Tracking #:432317593

Date:11-08-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the native SSH daemon of Erlang's Open Telecom Platform (OTP), which is being actively exploited in the wild. This flaw allows remote code execution (RCE), potentially leading to full system compromise.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-32433) has been identified in the Secure Shell (SSH) daemon of the Erlang programming language's Open Telecom Platform (OTP) that is being actively exploited in the wild. The flaw enables unauthenticated remote code execution (RCE) by allowing specially crafted SSH protocol messages (codes ≥ 80) to be processed before authentication, leading to arbitrary code execution without credentials.

Erlang/OTP is widely used in telecommunications, finance, 5G infrastructure, and industrial OT systems, amplifying the risk of exploitation in critical environments.

Vulnerability Details

- **CVE-2025-32433**
- CVSS Score 10.0 Critical
- **Vulnerability type:** Improper state enforcement in SSH daemon
- **Impact:** Unauthenticated RCE, potential full system compromise
- **Attack vector:** Network — sending malicious SSH protocol messages to an open Erlang/OTP SSH port
- **Notable ports:** Often on non-standard ports such as TCP/2222 (also used in industrial Ethernet/IP protocols)
- **Affected components:** Native Erlang/OTP SSH implementation, used for encrypted connections, file transfers, and command execution

The issue affects Erlang/OTP versions:

- **OTP-27:** prior to 27.3.3
- **OTP-26:** prior to 26.2.5.11
- **OTP-25:** prior to 25.3.2.20

Indicators of Compromise (IOCs):

- .dns.outbound.watchtowr[.]com
- 194.165.16[.]71
- 146.103.40[.]203

RECOMMENDATIONS:

- Upgrade Erlang/OTP to OTP-27.3.3, OTP-26.2.5.11, or OTP-25.3.2.20 (or later).
- Disable Erlang/OTP SSH service if not required.
- Restrict SSH access to trusted IP addresses via firewall rules.
- Inspect logs for anomalous SSH protocol messages pre-authentication.
- Monitor for IOCs in DNS, firewall, and endpoint logs.
- Enhance IT/OT segmentation to reduce cross-environment compromise potential.
- Deploy intrusion prevention updates for known exploit signatures.
- Regularly audit exposed OT endpoints on non-standard ports.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://unit42.paloaltonetworks.com/erlang-otp-cve-2025-32433/
- https://nvd.nist.gov/vuln/detail/CVE-2025-32433