NCSC Advisory

Critical Vulnerability in the Erlang/Open Telecom Platform SSH Implementation
CVE-2025-32433

23rd, April 2025

STATUS: TLP:CLEAR

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Description

CVE ID: CVE-2025-32433

Published: 2025-04-16

Vendor: Erlang

Product: OTP

CVSS Score[1]: 10.0

Products Affected

Product	Version
OTP	>= OTP-27.0-rc1, < OTP-27.3.3
OTP	>= OTP-26.0-rc1, < OTP-26.2.5.11
OTP	< OTP-25.3.2.20

Impact

Erlang/Open Telecom Platform (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 unauthorised 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.

Common Weakness Enumeration (CWE)[2]: CWE-306: Missing Authentication for Critical Function

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

---

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Erlang.

- https://nvd.nist.gov/vuln/detail/CVE-2025-32433

- https://www.cve.org/CVERecord?id=CVE-2025-32433

- https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2

- https://github.com/erlang/otp/commit/0fcd9c56524b28615e8ece65fc0c3f66ef6e4c12

- https://github.com/erlang/otp/commit/6eef04130afc8b0ccb63c9a0d8650209cf54892f

- https://github.com/erlang/otp/commit/b1924d37fd83c070055beb115d5d6a6a9490b891

- http://www.openwall.com/lists/oss-security/2025/04/16/2

- http://www.openwall.com/lists/oss-security/2025/04/18/1

- http://www.openwall.com/lists/oss-security/2025/04/18/2

- http://www.openwall.com/lists/oss-security/2025/04/18/6

- http://www.openwall.com/lists/oss-security/2025/04/19/1

- https://github.com/ProDefense/CVE-2025-32433/blob/main/CVE-2025-32433.py

Tom Johnson House, Beggar's Bush, Dublin 4, Ireland, D04 K7X4
T +353 (0)1 678 2333   **E** info@ncsc.gov.ie

ncsc.gov.ie

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

TLP: CLEAR