



An Láirionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2504230134

NCSC Advisory

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

23rd, April 2025

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2025-32433**Published:** 2025-04-16**Vendor:** Erlang**Product:** OTP**CVSS Score¹:** 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) catalog³: 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>



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>

