Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Erlang/OTP SSH Flaw Lets Hackers Bypass Login and Run Code

Date of Publication	Last Updated Date	Admiralty Code	TA Number
April 21, 2025	August 12, 2025	A1	TA2025121

Summary

First Seen: April 16, 2025
Affected Product: Erlang/OTP
Targeted Countries: United States, Japan, Brazil, France, Netherlands, Ireland, Ecuador
Targeted Industries: Education, Healthcare, Agriculture, Media & Entertainment, High Technology, Telecommunications, Financial services
Impact: CVE-2025-32433 is a critical unauthenticated remote code execution vulnerability in the Erlang/OTP SSH server, rated CVSS 10.0 for its maximum severity. It allows attackers to execute arbitrary commands without valid credentials by exploiting improper handling of SSH messages before authentication. The bug is already being exploited in the wild, targeting OT networks and sectors like education, healthcare, and telecom, with proof-of-concept code publicly available. Users should patch immediately or restrict SSH access to mitigate risk.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-32433	Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability	Erlang/OTP	✗	✓	✓

Vulnerability Details

#1

CVE-2025-32433 is a critical vulnerability in the SSH server component of the Erlang/OTP programming platform that allows unauthenticated remote code execution. An attacker can take full control of a vulnerable server simply by sending specially crafted SSH messages—no username, password, or prior access is required. The flaw is particularly dangerous because it is exploited before any authentication takes place, meaning even systems with strong credentials are still exposed. It stems from a flaw in how Erlang/OTP's SSH server processes certain message types, incorrectly handling some requests without verifying the user first.

#2

The vulnerability affects widely deployed Erlang/OTP versions prior to OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. Erlang/OTP is frequently used in backend systems for messaging platforms, telecom infrastructure, IoT devices, and industrial control systems, making the potential attack surface extensive. Because these environments are often high-performance and always online, exploitation could lead to severe consequences ranging from data theft to service disruption. Researchers have already published proof-of-concept exploit code, confirming the ease of attack on unpatched systems.

#3

Active exploitations began as early as May 2025, with most attempts targeting operational technology (OT) networks—particularly those in the U.S., Japan, Brazil, France, the Netherlands, Ireland, and Ecuador. The education sector alone accounted for over 72% of all exploit detections. Attackers often delivered reverse shells and used DNS-based callbacks (such as gethostbyname lookups to randomized domains) to verify successful code execution without raising immediate alarms. The attacks were not constant but came in short bursts, peaking on specific dates, suggesting coordinated campaigns.

#4

The combination of unauthenticated execution, ease of exploitation, and the availability of working exploit code makes CVE-2025-32433 a high-priority risk for any organization running affected Erlang/OTP versions. The threat is amplified in OT and IoT contexts, where compromise could have physical-world impacts. Industrial systems running Erlang/OTP SSH services on ports like 2222, 830, or 2022 are especially exposed. The ongoing convergence of IT and OT systems means even non-industrial sectors may host vulnerable services in overlooked parts of their infrastructure.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-32433	All Erlang/OTP SSH servers running versions: OTP-27.3.2 and earlier OTP-26.2.5.10 and earlier OTP-25.3.2.19 and earlier	cpe:2.3:a:erlang:otp:*:*:*:*:*:*:*:*	CWE-306

Recommendations

Update Erlang/OTP Immediately: Upgrade to fixed versions OTP-27.3.3, OTP-26.2.5.11, or OTP-25.3.2.20 immediately. Check your current version by running erl +V or using your system's package manager.

Restrict SSH Access: If you can't update right away, limit who can access the SSH server. Use firewalls or network rules to allow only trusted IP addresses to connect to the server. This can reduce the chance of someone exploiting the flaw from the internet.

Disable Erlang's SSH Server (Temporarily): If the Erlang/OTP SSH server isn't absolutely necessary for your setup, consider disabling it until you can apply the patch. Use a different, secure SSH server if needed.

Monitor Logs and Traffic: Watch for unusual SSH traffic or signs of unauthorized access. Attackers may try scanning for vulnerable servers, and early detection can help prevent full exploitation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0008 Lateral Movement	TA0043 Reconnaissance	TA0011 Command and Control
T1210 Exploitation of Remote Services	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities
T1078.001 Default Accounts	T1078 Valid Accounts	T1203 Exploitation for Client Execution	T1588 Obtain Capabilities
T1595 Active Scanning	T1071.004 DNS	T1071 Application Layer Protocol	T1021 Remote Services
T1588.005 Exploits	T1068 Exploitation for Privilege Escalation		

Indicators of Compromise (IOCs)

TYPE	VALUE
Hostname	[.]dns[.]outbound[.]watchtowr[.]com
IPv4	194[.]165[.]16[.]71, 146[.]103[.]40[.]203

Patch Details

Upgrade Erlang/OTP immediately to version OTP-27.3.3, OTP-26.2.5.11, or OTP-25.3.2.20 to patch the vulnerability.

Links:
https://github.com/erlang/otp/releases

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

References

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

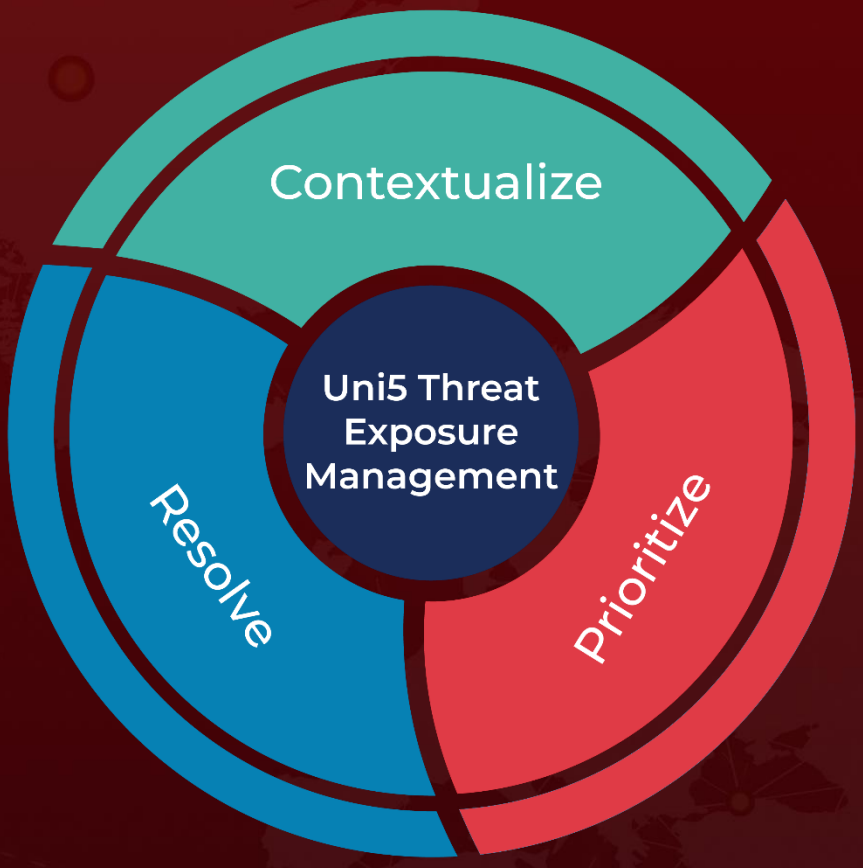
https://platformsecurity.com/blog/CVE-2025-32433-poc

https://unit42.paloaltonetworks.com/erlang-otp-cve-2025-32433/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 21, 2025 • 4:30 AM

More at www.hivepro.com