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	Admiralty Code	TA Number
April 21, 2025	A1	TA2025121

Summary

First Seen: April 16, 2025
Affected Product: Erlang/OTP
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. Affected systems are highly exposed to takeover. 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/OTP Unauthenticated Remote Code Execution Vulnerability	Erlang/OTP	✗	✓	✓

Vulnerability Details

#1

CVE-2025-32433 is a critical vulnerability found in the SSH server component of the Erlang/OTP programming platform. It allows an attacker to run code on a system without needing to log in first. This means someone could take full control of a server just by sending it specially crafted SSH messages. The flaw is especially dangerous because it works before any authentication takes place, so the attacker doesn't need a username or password.

#2

The issue comes from how the Erlang/OTP SSH server processes certain messages. Normally, a server should only handle commands after a user is verified. But in this case, it accepts and processes some types of requests even if the user hasn't logged in yet. Attackers can take advantage of this by sending a message that includes malicious code, which the server then executes.

#3

This vulnerability affects multiple versions of Erlang/OTP specifically, versions before OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. These versions are widely used in backend systems for messaging apps, telecom infrastructure, and IoT devices, which means the potential impact is large. Because Erlang is often used in high-performance, always-online environments, attackers could target these systems for data theft or to disrupt services.

#4

Researchers have even published a proof-of-concept exploit to show how easy it is to attack unpatched systems, so the threat is real and urgent. To stay protected, users should update their Erlang/OTP installations to one of the patched versions immediately. If updating isn't possible right away, temporarily blocking access to the SSH server or disabling it can reduce the risk.

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	T1588.005 Exploits	T1068 Exploitation for Privilege Escalation
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

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

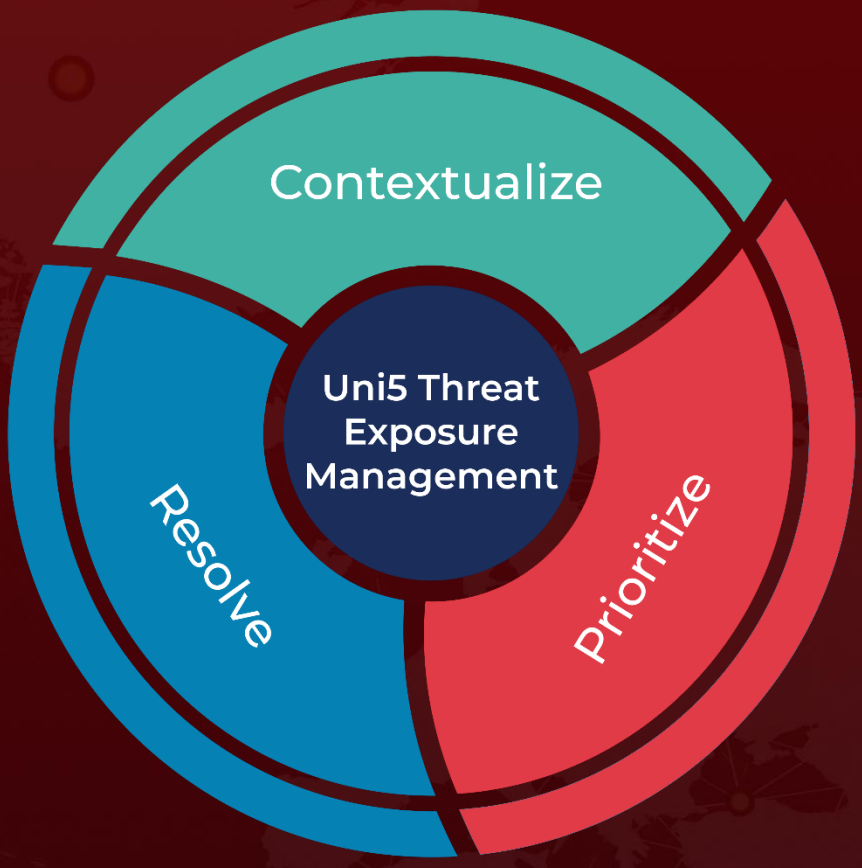
https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2

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

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