Erlang/OTP SSH Vulnerability Sees Spike in Exploitation Attempts

Data: 2025-08-13 16:45:00

Autor: Inteligência Against Invaders

A severe remote code execution (RCE) vulnerability in Erlang's Open Telecom Platform (OTP)

Secure Shell daemon (sshd) is being actively exploited.

According to a new analysis by Palo Alto's Unit 42, CVE-2025-32433, rated 10.0 on the CVSS scale, allows unauthenticated attackers to execute commands by sending specific SSH messages before authentication.

Vulnerable versions include Erlang/OTP releases before OTP-27.3.3, OTP-26.2.5.11 and OTP-25.3.2.20.

Surge in Targeted Attacks

Between May 1 and May 9, the researchers observed a surge in exploitation attempts, with 70% of detections originating from firewalls protecting operational technology (OT) networks.

Many targeted sectors rely on Erlang/OTP's native SSH for remote administration, including healthcare, agriculture, media and entertainment and high technology.

"This vulnerability, if exploited, could have severe consequences on the organization, their network and operations,"said Thomas Richards, infrastructure security practice director at Black Duck.

"The attacker would have full control over the system, which can result in a compromise of sensitive information and allow them to compromise additional hosts within the network."

Erlang/OTP services were found to be widely exposed on the internet, sometimes over industrial ports like TCP 2222, creating a crossover risk between IT and industrial control systems. The US, Brazil and France host the highest number of exposed services.

Read more on operational technology security: Over Half of Organizations Report Serious OT Security Incidents

Exploitation Details and Mitigation

Attackers have been observed deployingpayloads that establish reverse shells for unauthorized access.

One method binds a shell to a TCP connection, whileanother redirects Bash input and output to a

remote host linked to botnet command servers. Some payloads utilize DNS callbacks to track execution without returning results –a tactic commonly employed in stealthy campaigns.

“The real danger with CVE-2025-32433 is that it’s not just an IT vulnerability: it is disproportionately affecting [OT] networks, and it’s already actively showing up in systems tied to critical infrastructure.”said April Lenhard, principal product manager at Qualys.

According to Lenhard,exploitation could “alter sensor readings, trigger outages, introduce safety risks and cause physical damage.”

While education accounted for 72.7% of all detections, many OT-heavy sectors like utilities, mining and aerospace saw no recorded OT triggers, possibly due to segmentation, delayed targeting or gaps in detection.

Researchers urge organizations to patch immediately, upgradingto OTP 27.3.3, OTP 26.2.5.11 or OTP 25.3.2.20. Temporary measures include disabling the SSH server or restricting access via firewall rules.

“Addressing this vulnerability should be a top priority for any security team responsible for an OT network,”Richards concluded.