

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Authentication Bypass Vulnerability in Teleport

Tracking #:432317406

Date:24-06-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability, tracked as CVE-2025-49825, has been discovered in Teleport, an open-source platform used for secure access to servers, cloud applications, and infrastructure.

TECHNICAL DETAILS:

A critical security vulnerability, tracked as CVE-2025-49825, has been discovered in Teleport, an open-source platform used for secure access to servers, cloud applications, and infrastructure. The flaw enables remote attackers to bypass SSH authentication controls, potentially allowing unauthorized access to critical systems across both self-hosted and cloud-based environments.

The vulnerability affects multiple major versions of Teleport Community Edition and integrated deployments using Teleport SSH agents, OpenSSH, and Teleport Git proxies.

Vulnerability Details:

- CVE ID: CVE-2025-49825
- Severity: Critical (CVSS 9.8)
- Impact: Remote SSH Authentication Bypass
- Affected Products: Teleport Community Edition
- Affected Versions:
 - < 17.5.2
 - < 16.5.12
 - < 15.5.3
 - < 14.4.1
 - < 13.4.27
 - < 12.4.35
- Fixed Versions:
 - 17.5.2
 - 16.5.12
 - 15.5.3
 - 14.4.1
 - 13.4.27
 - 12.4.35
- Exploit Status: No known public exploit; no active exploitation detected
- Attack Vector: Remote (SSH, Git Proxy, Kubernetes)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to organizations using Teleport should upgrade to the latest patched versions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://github.com/gravitational/teleport/security/advisories/GHSA-8cqv-pj7f-pwpc>