مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Authentication Bypass Vulnerability in OpenSSH

Tracking #:432318860

Date:29-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-impact vulnerability (CVE-2026-35414) has been identified in OpenSSH, enabling a potential authentication bypass under specific conditions

TECHNICAL DETAILS:

A high-impact vulnerability (CVE-2026-35414) has been identified in OpenSSH versions prior to 10.3, enabling a potential authentication bypass under specific conditions. The flaw arises from improper handling of the authorized_keys principals option when used with certificate-based authentication and certain malformed principal names.
Successful exploitation could allow unauthorized users—possessing a valid certificate from a trusted Certificate Authority (CA)—to gain elevated access, potentially as root.

Vulnerability Details:

- CVE ID: CVE-2026-35414
- CVSS Score NIST (NVD): 8.1 (High)
- Affected Software: OpenSSH versions < 10.3
- Vulnerability Type: Authentication Bypass
- CWE Classification: CWE-670 (Always-Incorrect Control Flow Implementation)
- Fixed Versions: OpenSSH to version 10.3 or later

RECOMMENDATIONS:

- Immediate Actions: Upgrade OpenSSH to fixed version.

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://www.openssh.org/releasenotes.html#10.3p1