مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Remote code execution (RCE) Vulnerability in OpenSSH

Tracking #:432317794

Date:09-10-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in OpenSSH's ProxyCommand feature that could be exploited to achieve remote code execution on affected systems.

TECHNICAL DETAILS:

A security vulnerability (CVE-2025-61984) affecting OpenSSH before version 10.1 allows remote code execution when control characters—such as newlines—in usernames are mishandled by the ProxyCommand directive. This issue arises through insufficient input filtering, enabling attackers to inject and execute unintended commands in specific shell environments.

Vulnerability Details

- **CVE-2025-61984**
- CVSS Base Score: 3.6 LOW
- Attackers may exploit this vulnerability by crafting a malicious SSH username containing control characters (notably $, [, and newline), which, when passed into ProxyCommand using the %r token, results in malformed execution lines. Permissive shell interpreters (Bash, csh, fish) may continue parsing lines after a syntax error in the exec directive, leading to execution of additional attacker-controlled commands.
- Impact: Remote code execution (RCE) under certain configurations
- A public proof-of-concept (PoC) exploit is available

Affected Versions:

- OpenSSH versions prior to 10.1

Fixed Versions:

- OpenSSH versions 10.1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by OpenSSH.

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://nvd.nist.gov/vuln/detail/CVE-2025-61984