مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Update- OpenSSH

Tracking #:432319272

Date:09-07-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple security vulnerabilities have been addressed in newly released OpenSSH affecting both SSH clients and servers.

TECHNICAL DETAILS:

Multiple security vulnerabilities have been addressed in OpenSSH 10.4 (10.4p1), affecting both SSH clients and servers. The update resolves eight security issues, including a high-severity client-side use-after-free vulnerability (CVE-2026-60002) that could allow a malicious SSH server to crash or disrupt a connecting client during key re-exchange.

Additional vulnerabilities impact SFTP and SCP file transfer operations, allowing attacker-controlled servers to write downloaded files to unintended locations. Several server-side fixes also improve OpenSSH daemon (sshd) security by restoring authentication delays, strengthening forwarding restrictions, mitigating denial-of-service conditions, and improving internal validation.

Vulnerability Details:

- CVE-2026-60002 – High (CVSS 7.7) – Client-side use-after-free vulnerability that may cause a crash when a malicious SSH server changes its host key during key re-exchange.
- CVE-2026-59995 – Medium – SFTP path handling vulnerability allowing a malicious server to save downloaded files to unintended locations.
- CVE-2026-59996 – Medium – SCP path traversal vulnerability allowing a malicious server to write downloaded files into parent directories.
- CVE-2026-60001 – Medium – Authentication delay issue that weakens protection against brute-force login attempts.
- CVE-2026-59999 – Medium – Forwarding restriction issue where PermitTunnel could override DisableForwarding under certain conditions.
- CVE-2026-60000 – Medium – GSSAPI-related denial-of-service vulnerability that could allow a remote attacker to disrupt SSH services.

Affected Versions

- OpenSSH All versions prior to 10.4

Fixed Version

- OpenSSH 10.4 (10.4p1)

RECOMMENDATIONS:

Immediate Actions:

- Upgrade immediately OpenSSH to the latest vendor-supported release.

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.openwall.com/lists/oss-security/2026/07/06/5