مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

OpenSSH Pre-Authentication Vulnerability in FreeBSD

Tracking #:432316135

Date:12-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an OpenSSH pre-authentication vulnerability in OpenSSH that affects FreeBSD systems, allowing unauthenticated attackers to execute arbitrary code remotely.

TECHNICAL DETAILS:

Vulnerability Details:

- **Vulnerability Identifier**: **CVE-2024-7589**, CVSS v3- Base Score: 7.4
- **Type of Vulnerability**: Pre-authentication remote code execution (RCE)
- **Severity Level**: High
- **Cause:** Issue with a signal handler in the sshd daemon when clients fail authentication within the default LoginGraceTime of 120 seconds.
- **Risk:** Potential for unauthenticated remote code execution with root privileges.
- **Previous Relation**: Linked to earlier vulnerability CVE-2024-6387 concerning the integration of blacklistd.

Fixed Versions:

The FreeBSD Project recommends upgrading to a supported stable or release/security branch that includes the necessary patch to fix this vulnerability.

- FreeBSD OS 14.0
- FreeBSD OS 14.1
- FreeBSD OS 13.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by FreeBSD.

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.freebsd.org/security/advisories/FreeBSD-SA-24:08.openssh.asc