CYBER ADVISORY

TLP:CLEAR

12 August 2024

FreeBSD Vulnerability

CVE-2024-7589 | FreeBSD | OpenSSH | High Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high vulnerability known as CVE-2024-7589.[1] The vulnerability affects the OpenSSH, an implementation of Secure Shell (SSH) protocol suite, in all supported versions of FreeBSD.[2] Exploitation of the vulnerability may allow an unauthenticated attacker remote code execution (RCR) as root.[3]

The Cal-CSIC recommends applying upgrades or implementing workarounds as soon as possible.

For further information on applying upgrades or workarounds please refer to FreeBSD.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Security Affairs; "FreeBSD Project maintainers addressed a high-severity flaw in OpenSSH that could allow remote code execution with elevated privileges.;" https://securityaffairs.com/166941/security/freebsd-openssh-flaw.html; accessed 12 August 2024
[2] The Hacker News; "FreeBSD Releases Urgent Patch for High-Severity OpenSSH Vulnerability" https://thehackernews.com/2024/08/freebsd-releases-urgent-patch-for-high.html; accessed 12 August 2024
[3] CVE.ORG; "CVE-2024-7589" https://www.cve.org/CVERecord?id=CVE-2024-7589; accessed 12 August 2024