CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
01 July 2024

OpenSSH Race Condition Vulnerability

CVE-2024-6387 | OpenSSH | regreSSHion | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-6387.[1,2] The vulnerability affects OpenSSH versions earlier than 4.4p1 and versions between 8.5p1 and 9.7p1. Versions prior 4.4p1 are also vulnerable to the race condition bug unless they are patched for CVE-2006-5051 and CVE-2008-4109.[2,3] Named "regreSSHion" due to a previous flaw that has now reappeared in later versions, this exploitation is an unauthenticated remote code execution (RCE) that grants full root access.[2]

The Cal-CSIC recommends immediately upgrading to OpenSSH version 9.8p1.

For further information on applying upgrades please refer to OpenSSH.[4]

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.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

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] BleepingComputer; "New regreSSHion OpenSSH RCE bug gives root on Linux servers" https://www.bleepingcomputer.com/news/security/new-regresshion-openssh-rce-bug-gives-root-on-linux-servers/; accessed 01 July 2024

[2] Qualys; "The regreSSHion Bug" https://www.qualys.com/regresshion-cve-2024-6387/| Qualys; accessed 01 July 2024

[3] TheHackerNews; "New OpenSSH Vulnerability Could Lead to RCE as Root on Linux Systems" https://thehackernews.com/2024/07/new-openssh-vulnerability-could-lead-to.htmlaccess 01 July 2024

[4] OpenSSH 9.8; https://www.openssh.com/

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.