CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

TLP:CLEAR
07 February 2024

Shim Vulnerability

CVE-2023-40547 | Bootloader | RCE | Critical Vulnerability

The California Cyber Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2023-40547. The vulnerability affects all versions prior to Shim version 15.8, which is a critical piece of software used by most Linux distributions in the boot process to support Secure Boot. [1] The vulnerability stems from HTTP protocol handling, leading to an out-of-bounds write that may lead to complete system compromise via remote code execution (RCE).[2,3]

The Cal-CSIC recommends immediately upgrading to Shim version 15.8.

For further information on applying upgrades, please refer to Shim Version 15.8.

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.

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.

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] Eclypsium; "The Real Shim Shady - How Cve-2023-40547 Impacts Most Linux Systems;" https://eclypsium.com/blog/the-real-shim-shady-how-cve-2023-40547-impacts-most-linux-systems/; accessed 07 February 2024

[2] The Hacker News; "Critical Bootloader Vulnerability in Shim Impacts Nearly All Linux Distros;" https://thehackernews.com/2024/02/critical-bootloader-vulnerability-in.html; accessed 07 February 2024

[3] Ubuntu; "CVE-2023-40547;" https://ubuntu.com/security/CVE-2023-40547; accessed 07 February 2024

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.