CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

TLP:CLEAR
16 July 2024

HPE 3PAR Service Processor Software, Remote Bypass Vulnerability

CVE-2024-22442 Hewlett Packard Service Processor Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-22442.[1,2] The vulnerability affects HPE 3PAR Service Processor v5.1.1 and earlier. Exploiting CVE-2024-22442 allows remote authentication bypass capability;[2,3] enabling attackers to gain access to the Service Processor Software without the need for login credentials.

The Cal-CSIC recommends immediately upgrading to HPE 3PAR Service Processor v5.1.2. [3]

For further information on applying upgrades please refer to HPESBST04663 rev.1 - HPE 3PAR Service Processor Software, Remote Bypass Security Restriction Vulnerability.[3]

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] CVE.org; "CVE-2024-22442"; https://www.cve.org/CVERecord?id=CVE-2024-22442/; accessed 16 July 2024

[2] National Vulnerability Database; "CVE-2024-22442 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-22442; accessed 16 July 2024

[3] HPE Support; "HPESBST04663 rev.1 - HPE 3PAR Service Processor Software, Remote Bypass Security Restriction Vulnerability"; https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04663en_us&docLocale=en_US; accessed 16 July 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.