Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
05 March 2024

Multiple VMWare Vulnerabilities

CVE-2024-22252 | CVE-2024-22253 | VMWare | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple critical and high vulnerabilities known as CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255.[1] The vulnerabilities affect VMWare ESXi, Workstation, Fusion, and ESXi Cloud Foundation products.[2] The most critical vulnerabilities could allow a malicious actor with local admin privileges on a virtual machine to execute code as the virtual machine's VMX process running on the host.[3]

Product	Version	Running On	CVE Identifier	Fixed Version
ESXi	8.0	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	ESXi80U2sb-23305545
ESXi	8.0 [2]	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	ESXi80U1d-23299997
ESXi	7.0	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	ESXi70U3p-23307199
Workstation	17.x	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22255	17.5.1
Fusion	13.x	Mac OS	CVE-2024-22252, CVE-2024-22253, CVE-2024-22255	13.5.1
Cloud Foundation (ESXi)	5.x/4.x	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	KB88287

Table 1: VMWare Affected Products, Associated CVEs, and Upgraded Versions

The Cal-CSIC recommends upgrading the affected to product with the appropriate VMWare patch when possible.

For further information on applying upgrades, please refer to VMWare Customer Connect.

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.

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 Week; "VMware Patches Critical ESXi Sandbox Escape Flaws;" https://www.securityweek.com/vmware-patches-critical-esxi-sandbox-escape-flaws/?utm_source=dlvr.it; accessed 05 March 2024

[2] Vulnera; "Critical ESXi Sandbox Escape Vulnerabilities Addressed by VMware in Urgent Updates;" https://vulnera.com/newswire/critical-esxi-sandbox-escape-vulnerabilities-addressed-by-vmware-in-urgent-updates/; accessed 05 March 2024

[3] VMWare; "VMSA-2024-0006;" https://www.vmware.com/security/advisories/VMSA-2024-0006.html; accessed 05 March 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.