CYBER ADVISORY

TLP:CLEAR
29 July 2024

VMWare ESXi and Cloud Foundation Vulnerability

CVE-2024-37085 | ESXi | Cloud Foundation | Active Exploitation

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a moderate vulnerability under active exploitation known as CVE-2024-37085.[1] The vulnerability affects VMWare's ESXi hypervisor versions 7.0-8.0 and Cloud Foundation versions 4.x-5.x.[2] Exploitation of the vulnerability could allow an attacker with sufficient Active Directory (AD) permissions to gain full access to an ESXi host that was previously configured to use AD for user management by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.[3]

The Cal-CSIC recommends immediately applying workarounds or patches as applicable.

For further information on applying work arounds please refer to Secure Default Settings for ESXi Active Directory integration. For applying patches to VMware Cloud Foundation please refer to VMware Cloud Foundation 5.2. For applying patches to VMware ESXi please refer to VMware ESXi 8.0 Update 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.
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] Microsoft; "Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption;" https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/; accessed 29 July 2024

[2] Bleeping Computer; "Microsoft: Ransomware gangs exploit VMware ESXi auth bypass in attacks" https://www.bleepingcomputer.com/news/microsoft/microsoft-ransomware-gangs-exploit-vmware-esxi-auth-bypass-in-attacks/; accessed 29 July 2024

[3] Broadcom; "VMSA-2024-0013:VMware ESXi and vCenter Server updates address multiple security vulnerabilities (CVE-2024-37085, CVE-2024-37086, CVE-2024-37087)" https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505; accessed 29 July 2024