CYBER ADVISORY

TLP:CLEAR
21 November 2024

Broadcom Updates VMware vCenter Server Heap-Overflow and Privilege Escalation Vulnerabilities

CVE-2024-38812 | Heap-Overflow | CVE-2024-38813 | Privilege Escalation

---

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of an update for two vulnerabilities that are affecting VMware products. The first, CVE-2024-38812 has a CVSS v3.1 score of 9.8 and is rated critical. The second, CVE-2024-38813 has a CVSS v3.1 score of 7.5 and is rated high. Broadcom has warned these two previously disclosed vulnerabilities are now being exploited-in the-wild and has released an updated patch for CVE-2024-38812, but not CVE-2024-38813.[1]

Systems Affected:

- VMware vCenter Server
  Version 8.0, 7.0
- VMware Cloud Foundation
  Version 5.x, 5.1.x,4.x

CVE-2024-38812 is a heap-overflow vulnerability in the Distributed Computing Environment / Remote Procedure Call (DCERPC) protocol, allowing a threat actor with network access to potentially utilize remote code execution (RCE) via specially crafted network packets. [2]

CVE-2024-38813 is a privilege escalation flaw, in which a malicious actor with network access to a vCenter Server may trigger to further escalate privileges to root by sending a specially crafted network packet.[3]

The two vulnerabilities combined allow for a full-chain exploit. This can lead to full system takeover, lateral movement and persistent backdoor installation.

The Cal-CSIC recommends immediately applying the appropriate patches provided by Broadcom to the vulnerable systems.

For further information on applying these patches please refer to Broadcom Advisory.

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 here.
Source Summary Statement	**UPDATE THIS PORTION APPROPRIATELY**
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] Broadcom; "VMSA-2024-0019:VMware vCenter Server updates address heap-overflow and privilege escalation vulnerabilities (CVE-2024-38812, CVE-2024-38813)"; https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968; accessed 20 November 2024

[2] National Vulnerability Database; "CVE-2024-38812 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-38812; accessed 20 November 2024

[3] National Vulnerability Database; "CVE-2024-38813 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-38813; accessed 20 November 2024