CYBER ADVISORY

TLP:CLEAR
22 May 2024

Veeam Backup Enterprise Manager Vulnerability

Veeam | VBEM | CVE-2024-29849 | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-29849.[1] The vulnerability lies in Veeam Backup Enterprise Manager (VBEM), a supplementary application customers may deploy to manage Veeam Backup & Replication using a web console.[2] Exploitation of the vulnerability may allow an attacker to bypass authentication protections and log in to the VBEM web interface as any user. [3]

The Cal-CSIC recommends to immediately upgrade to the appropriate Veeam Backup & Replication build number.

For further information on applying Veeam updates, please refer to Release Information for Veeam Backup & Replication Updates.

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] The Hacker News; "Critical Veeam Backup Enterprise Manager Flaw Allows Authentication Bypass;" https://thehackernews.com/2024/05/critical-veeam-backup-enterprise.html; accessed 22 May 2024

[2] Tenable; "CVE-2024-29849;" https://www.tenable.com/cve/CVE-2024-29849; accessed 22 May 2024

[3] Veeam; "Veeam Backup Enterprise Manager Vulnerabilities;" https://www.veeam.com/kb4581; accessed 22 May 2024