# CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

*CYBER ADVISORY*

TLP:CLEAR
10 SEP 2024

## Veeam Multiple Vulnerabilities

Veeam | multiple CVEs | Remote Code Execution | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple vulnerabilities affecting multiple Veeam products. Exploitation of these vulnerabilities could potentially allow an attacker the ability to gain full control of a system, manipulate data, and/or potentially move laterally within a network.[1]

| Affected Product | Issue | CVE Identifier(s) | CVSS v3.1 |
|---|---|---|---|
| **Veeam Backup & Replication 12.1.2.172 and all earlier version 12 builds.** | A vulnerability allowing unauthenticated remote code execution (RCE). | **CVE-2024-40711** | **9.8 Critical** |
| | A vulnerability that allows a user who has been assigned a low-privileged role within Veeam Backup & Replication to alter Multi-Factor Authentication (MFA) settings and bypass MFA. | **CVE-2024-40713** | **8.8 High** |
| | A series of related high-severity vulnerabilities, the most notable enabling remote code execution (RCE) as the service account and extraction of sensitive information (saved credentials and passwords). Exploiting these vulnerabilities requires a user who has been assigned a low-privileged role within Veeam Backup & Replication. | **CVE-2024-40710** | **8.8 High** |
| | A vulnerability that allows a low-privileged user to remotely remove files on the system with | **CVE-2024-39718** | **8.1 High** |

**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.

| | | | |
|---|---|---|---|
| | permissions equivalent to those of the service account. | | |
| | A vulnerability in TLS certificate validation allows an attacker on the same network to intercept sensitive credentials during restore operations. | **CVE-2024-40714** | **8.3 High** |
| | A path traversal vulnerability allows an attacker with a low-privileged account and local access to the system to perform local privilege escalation (LPE). | **CVE-2024-40712** | **7.8 High** |
| **Veeam Agent for Linux 6.1.2.1781 and all earlier version 6 builds.** | A vulnerability that allows a local low-privileged user on the machine to escalate their privileges to root level. | **CVE-2024-40709** | **7.8 High** |
| **Veeam ONE 12.1.0.3208 and all earlier version 12 builds.** | A vulnerability that allows an attacker in possession of the Veeam ONE Agent service account credentials to perform remote code execution on the machine where the Veeam ONE Agent is installed. | **CVE-2024-42024** | **9.1 Critical** |
| | A vulnerability that allows an attacker to access the NTLM hash of the Veeam Reporter Service service account. This attack requires user interaction and data collected from Veeam Backup & Replication. | **CVE-2024-42019** | **9.0 Critical** |
| | A vulnerability that allows low-privileged users to execute code with Administrator privileges remotely. | **CVE-2024-42023** | **8.8 High** |
| | A vulnerability that allows an attacker with valid access tokens to access saved credentials. | **CVE-2024-42021** | **7.5 High** |
| | A vulnerability that allows an attacker to modify product configuration files. | **CVE-2024-42022** | **7.5 High** |

| | | | |
|---|---|---|---|
| | A vulnerability in Reporter Widgets that allows HTML injection. | **CVE-2024-42020** | **7.3 High** |
| **Veeam Service Provider Console 8.0.0.19552 and all earlier version 8 builds.** | A vulnerability that allows a low privileged attacker to access the NTLM hash of service account on the VSPC server. | **CVE-2024-38650** | **9.9 Critical** |
| | A vulnerability that permits a low-privileged user to upload arbitrary files to the server, leading to remote code execution on VSPC server. | **CVE-2024-39714** | **9.9 Critical** |
| | A vulnerability that allows a low-privileged user with REST API access granted to remotely upload arbitrary files to the VSPC server using REST API, leading to remote code execution on VSPC server. | **CVE-2024-39715** | **8.5 High** |
| | A vulnerability that permits a low-privileged user to overwrite files on that VSPC server, which can lead to remote code execution on VSPC server. | **CVE-2024-38651** | **8.5 High** |
| **Veeam Backup for Nutanix AHV Plug-In 12.5.1.8 and all earlier version 12 builds.**<br>**Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization Plug-In 12.4.1.45 and all earlier version 12 builds.** | A vulnerability that allows a low-privileged user to perform local privilege escalation through exploiting an SSRF vulnerability. | **CVE-2024-40718** | **8.8 High** |

**Table 1: Vulnerable Veema Products[2]**

The Cal-CSIC recommends immediately upgrading all affected to the latest Patched Version listed below:[3]

- Veeam Backup & Replication Version: 12.2.0.334
- Veeam Agent for Linux Version: 6.2
- Veeam ONE 12.1.0.3208 Version: 12.2.0.4093
- Veeam Service Provider Console Version: 8.1.0.21377
- Veeam Backup for Nutanix AHV Version: 6.0.0.1228
- Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization Version: 12.5.0.299

For further information on upgrading affected Veema products, please refer to Veema | Latest 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] Help Net Security; “Veeam Backup & Replication RCE flaw may soon be leveraged by ransomware gangs (CVE-2024-40711);” https://www.helpnetsecurity.com/2024/09/09/cve-2024-40711-exploited/; accessed 10 September 2024

[2] Veeam; “Veeam Security Bulletin (September 2024);” https://www.veeam.com/kb4649; accessed 10 September 2024

[3] Veema; “Latest Updates;” https://www.veeam.com/products/downloads/latest-version.html; accessed 10 September 2024