Veeam Backup Enterprise Manager Vulnerabilities

May 2024

SOC Informative Report

Document details

Title of the activity
Veeam Backup Enterprise Manager Vulnerabilities

Summary
Report containing information about different vulnerabilities detected in the product Veeam Backup Enterprise Manager (VBEM), categorized as *Authentication bypass*.

Target audience
SOC and SOC AdS representatives

Confidentiality level (Clear/Green/Amber/Amber+Strict/Red)
CLEAR

Publication date
24/05/2024

Written by
Mirko Ioris, Luca Zeni

Reviewed by
Massimo Giaimo

Confidentiality level

A level of confidentiality is applied to the document, marked by the "Confidentiality Level" item on the front page. The values that can be used (RED / AMBER / AMBER+STRICT / GREEN / CLEAR) have the following meanings:

TLP:RED = Reserved for participants only.

> Sources may use TLP:RED when the information cannot be effectively used by other parties and could impact a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with parties outside the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most cases, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

TLP:AMBER+STRICT limits sharing to the *organization* only.

> Sources may use TLP:AMBER when the information requires support to act effectively but poses risks to privacy, reputation, or operations if shared outside the organizations involved. Recipients may share TLP:AMBER information only with members of their own organization and with clients or customers who need to know the information to protect themselves or prevent further harm.
>
> Note: If the source wishes to limit sharing **only** to the organization, it must specify TLP:AMBER+STRICT.

TLP:GREEN =Limited disclosure, restricted to the community.

> Sources may use TLP:GREEN when the information is useful for the awareness of all participating organizations, as well as with colleagues within the community or broader sector. Recipients may share TLP:GREEN information with colleagues and partner organizations within their sector or community, but not through publicly accessible channels. Information in this category may be widely disseminated within a particular community. TLP:GREEN information may not be released outside the community.

TLP:CLEAR = Disclosure is not limited.

Sources may use TLP:CLEAR when the information poses little or foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

Table of contents

Introduction

These vulnerabilities were discovered in **Veeam Backup Enterprise Manager (VBEM)**, a supplementary application customers may deploy to manage **Veeam Backup & Replication (VBR)** using a web console.

One of them is critical and allows an **unauthenticated attacker** to log in to the Veeam Backup Enterprise Manager web interface as any user.

Veeam Backup Enterprise Manager is a centralized tool for managing and controlling backup and recovery across multiple Veeam Backup & Replication environments.

It offers a unified dashboard to monitor backup health, manage jobs, and generate reports on system performance and storage use. The tool supports role-based access control, ensuring users have appropriate permissions, and features a federated search for easy data recovery. It also includes a self-service portal for user-initiated restores and supports multi-tenancy for service providers.

The following is a table containing the details of the vulnerabilities [1]:

CVE Number	CVSS Score	EPSS Score
CVE-2024-29849[2]	9.8 (Critical)	0.04% (Low)
CVE-2024-29850[3]	8.8 (High)	0.04% (Low)
CVE-2024-29851[4]	7.2 (High)	0.04% (Low)
CVE-2024-29852[5]	2.7 (Low)	0.04% (Low)

The EPSS associated with the vulnerabilities is very low at the time of writing this report (24/05/24) because the discoveries are new and not yet exploited, but might increase in the following weeks. There is no evidence of an exploit available in the wild.

Overview of the CVEs

CVE-2024-29849

This vulnerability in Veeam Backup Enterprise Manager allows an unauthenticated attacker to log in to the Veeam Backup Enterprise Manager web interface as any user. It has critical severity and a CVSS score of **9.8**. Since it's not yet exploited the associated EPSS score is low.

CVE-2024-29850

This high-severity vulnerability presents a dangerous vector for account takeover through NTLM relay. In environments where NTLM authentication is utilized, this vulnerability could allow attackers to intercept and relay authentication sessions, effectively granting them unauthorized access to the VBEM system. For this reason the CVSS score is **8.8** and the EPSS is 0.04%.

CVE-2024-29851

This vulnerability in Veeam Backup Enterprise Manager allows a high-privileged user to steal the NTLM hash of the Veeam Backup Enterprise Manager service account if that service account is anything other than the default Local System account. The CVSS score is **7.2** and no evidence of exploitation was found in the wild.

CVE-2024-29852

This vulnerability in Veeam Backup Enterprise Manager allows high-privileged users to read backup session logs. Since it only provides the ability to read session logs and nothing else, this CVE has the lowest CVSS score (**2.7**).

Remediation

The affected versions of the product are the following:

Veeam Backup & Replication |5.0|6.1|6.5|7.0|8.0|9.0|9.5|10|11|12|12.1

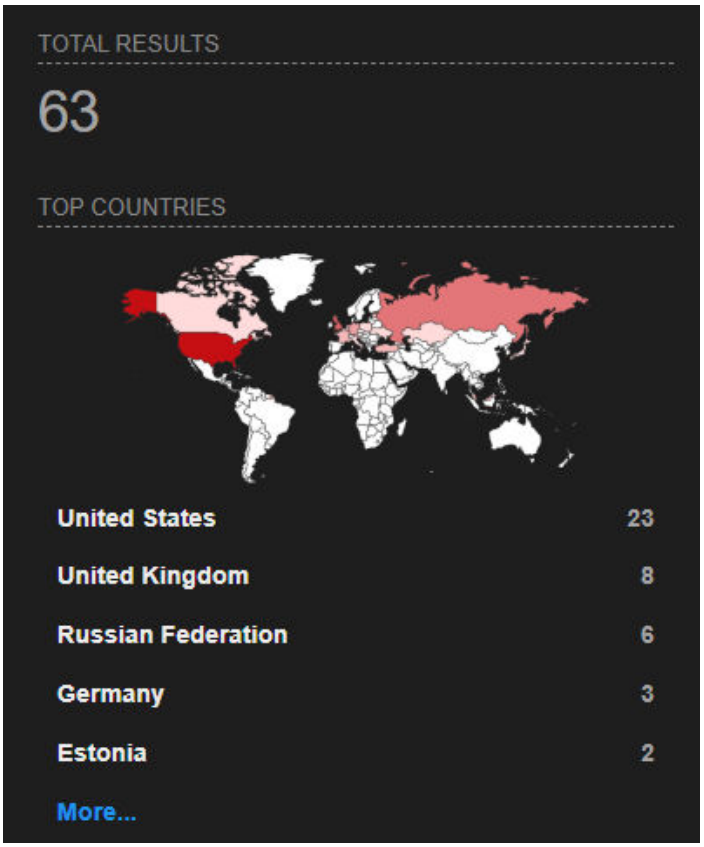
Veeam fixed all these vulnerabilities in the Veeam Backup Enterprise Manager **12.1.2.172 version**. It's strongly recommended to upgrade to the latest version if you are using VBEM.

If the update is not possible, network administrators can mitigate the threat by halting the Veeam Backup Enterprise Manager software. To do so it's sufficient to stop and disable the **VeeamEnterpriseManagerSvc** (Veeam Backup Enterprise Manager) and **VeeamRESTSvc** (Veeam RESTful API) services.

Attack surface

A quick search on Shodan returns “only” 63 exposed instances of VBEM that may be vulnerable if not patched. Most of them are located in the US [6].

Below are the devices found with the Shodan query (“http.title:"Veeam Backup Enterprise Manager", search date 24/05/2024):

Shodan Query
Veeam Backup Enterprise Manager


Bibliography

[1]https://www.veeam.com/kb4581

[2]https://nvd.nist.gov/vuln/detail/CVE-2024-29849

[3]https://nvd.nist.gov/vuln/detail/CVE-2024-29850

[4]https://nvd.nist.gov/vuln/detail/CVE-2024-29851

[5]https://nvd.nist.gov/vuln/detail/CVE-2024-29852

[6]https://www.neteye-blog.com/2024/05/soc-news-may-24-patch-now-this-veeam-critical-vulnerability/