

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Veeam Addresses Critical Flaws, Urges Admins to Patch

Date of Publication

June 11, 2024

Admiralty Code

A1

TA Number

TA2024224










Summary

Discovered: May 2024

Affected Products: Veeam Backup Enterprise Manager

Impact: Veeam has released fixes to address multiple security flaws affecting Veeam Backup Enterprise Manager. Among these vulnerabilities, CVE-2024-29849 is rated as critical with a CVSS score of 9.8. A proof of concept (PoC) for this vulnerability is now available. Successful exploitation could allow an unauthenticated attacker to log in to the Veeam Backup Enterprise Manager web interface as any user.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-29849	Veeam Backup Enterprise Manager Authentication Bypass Vulnerability	Veeam Backup Enterprise Manager			
CVE-2024-29850	Veeam Backup Enterprise Manager Authentication Replay Vulnerability	Veeam Backup Enterprise Manager			
CVE-2024-29851	Veeam Backup Enterprise Manager Privilege Escalation Vulnerability	Veeam Backup Enterprise Manager			

Vulnerability Details

#1

Veeam recently addressed several security vulnerabilities in its Backup and Replication software, ensuring enhanced protection for users. Of particular concern is CVE-2024-29849, which is classified as critical with a high severity score of 9.8. There's even a proof of concept (PoC) available, underlining the urgency of addressing this issue. Veeam Backup & Replication is widely regarded as a top-tier solution for data backup, recovery, and security.

#2

CVE-2024-29849 is a critical flaw that affects the authentication mechanism of the Veeam Backup Enterprise Manager web interface. Essentially, it allows unauthorized access for attackers who exploit a gap in authorization. By sending a specially crafted VMware single-sign-on (SSO) token to the Veeam API, attackers can gain entry without proper authentication. The existence of a PoC heightens the urgency for users to update their systems promptly.

#3

CVE-2024-29850 which is rated 8.8 on the CVSS scale, this vulnerability enables attackers to execute an account takeover using an NTLM relay attack. By tricking users into interacting with a malicious website or file, attackers can capture their NTLM hash, bypassing authentication.

#4

CVE-2024-29851 vulnerability, with a CVSS score of 7.2, allows high-privileged users to pilfer the NTLM hash of the Veeam Backup Enterprise Manager service account. This could potentially lead to privilege escalation if the compromised account isn't the default Local System account.

#5

All these vulnerabilities have been addressed in the latest version of Veeam Backup Enterprise Manager (12.1.2.172). Administrators are strongly urged to update their systems promptly to the latest version to mitigate these risks effectively. Notably, if Veeam Backup Enterprise Manager is installed on a dedicated server, it can be upgraded to the fixed version without the necessity of immediately upgrading Veeam Backup & Replication.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-29849	Veeam Backup Enterprise Manager versions before prior to 12.1.2.172	cpe:2.3:a:veeam:veeam_backup_&_replication:*:*:*:*:*	CWE-862
CVE-2024-29850	Veeam Backup Enterprise Manager versions before prior to 12.1.2.172	cpe:2.3:a:veeam:veeam_backup_&_replication:*:*:*:*:*	CWE-294
CVE-2024-29851	Veeam Backup Enterprise Manager versions before prior to 12.1.2.172	cpe:2.3:a:veeam:veeam_backup_&_replication:*:*:*:*:*	CWE-294

Recommendations



Update: Update to version 12.1.2.172 for Veeam Backup Enterprise Manager to address the vulnerabilities CVE-2024-29849, CVE-2024-29850, CVE-2024-29851.



Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.



Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.



Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0004 Privilege Escalation	TA0006 Credential Access
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1190 Exploit Public-Facing Application
T1539 Steal Web Session Cookie			

🛡️ Patch Details

Update your Veeam Backup Enterprise Manager to version 12.1.2.172. This update addresses all identified vulnerabilities, including CVE-2024-29849, CVE-2024-29850 and CVE-2024-29851.

Links:

<https://www.veeam.com/kb4510>

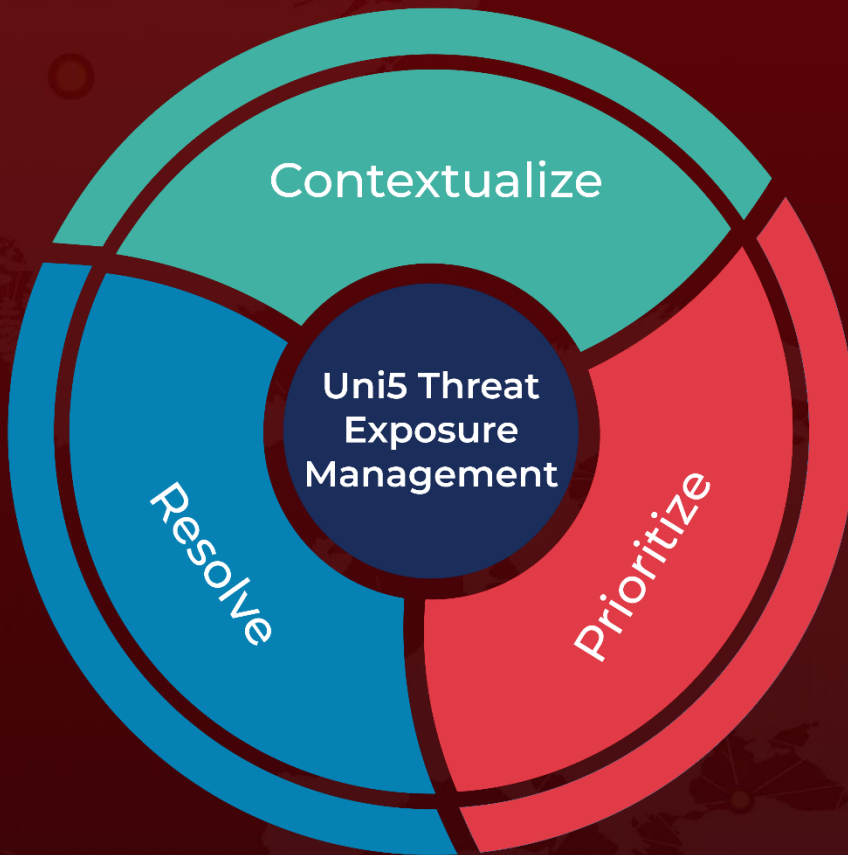
References

<https://www.veeam.com/kb4581>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

June 11, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com