**Security Advisory 2024-048**

# Critical Vulnerability in Veeam Backup Enterprise Manager

***May 22, 2024 — v1.0***

**TLP:CLEAR**

*History:*

- *22/05/2024 — v1.0 – Initial publication*

## Summary

On May 21, 2024, Veeam issued fixes addressing multiple security flaws in Veeam Backup Enterprise Manager, including a critical vulnerability allowing unauthenticated attackers to bypass authentication and gain access to the web interface as any user.

## Technical Details

The vulnerability `CVE-2024-29849`, with a CVSS score of 9.8, could allow an unauthenticated attacker to login into the Veeam Backup Enterprise Manager web interface as any user. The flaw lies in the authentication mechanism of the web interface.

The vulnerability `CVE-2024-29850`, with a CVSS score of 8.8, could allow account takeover via NTLM relay.

The vulnerability `CVE-2024-29851`, with a CVSS score of 7.2, could allow 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.

## Affected Products

Veeam Backup Enterprise Manager versions before prior to `12.1.2.172` are affected.

## Recommendations

It is strongly advised upgrading to the latest version as soon as possible.

### Workaround

For customers who are unable to upgrade Veeam Backup Enterprise Manager immediately, it is possible to mitigate these vulnerabilities by halting the Veeam Backup Enterprise Manager software.

To do so, the following services should be stopped and disabled:

- VeeamEnterpriseManagerSvc (Veeam Backup Enterprise Manager);
- VeeamRESTSvc (Veeam RESTful API Service).

## References

[1] https://thehackernews.com/2024/05/critical-veeam-backup-enterprise.html

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