ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about several critical vulnerabilities present in Veeam Backup Enterprise Manager.

Summary

On the 21st of May, Veeam published four critical vulnerabilities affecting an optional application for Veeam Backup & Replication. These vulnerabilities affect the Veeam Backup Enterprise Manager, a web-based console meant for easier management of Veeam Backup & Replication.[1]

These vulnerabilities are:

- CVE-2024-29849
  - Allows an unauthenticated attacker to log in to the Veeam Backup Enterprise Manager web interface as any user;
  - CVE score: 9.8
- CVE-2024-29850
  - allows account takeover via NTLM relay;
  - CVE score: 8.8
- CVE-2024-29851
  - 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;
  - CVE score: 7.2
- CVE-2024-29852
  - allows high-privileged users to read backup session logs.
  - CVE score: 2.7

Recommendations

Recommendation #1: Update as soon as possible

ORNA **strongly recommends** that organizations exposed to these vulnerabilities update their application as soon as possible to versions 12.1.2.172 or later.[2]

Recommendation #2: Mitigate until update is possible

ORNA **strongly recommends** that organizations unable to update as soon as possible, mitigate the vulnerabilities by halting the Veeam Backup Enterprise Manager software or uninstalling it if not in use.

Recommendation #3: Stay up to date

Monitor official channels to stay informed and updated on the situation involving security vulnerabilities.

References

1. https://www.veeam.com/kb4581
2. https://www.veeam.com/kb4510

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team