Multiple Vulnerabilities in Veeam ONE

Severity Level: High

Components Affected

- Veeam ONE 11
- Veeam ONE 11a
- Veeam ONE 12

Overview

Multiple vulnerabilities were identified in Veeam ONE IT Monitoring Software. An unauthenticated user could exploit some of these vulnerabilities to trigger elevation of privilege, remote code execution and sensitive information disclosure on the targeted system.

Description

Veeam ONE has several vulnerabilities which are described by their CVE number below:

- CVE-2023-38547 - Allows an unauthenticated user to gain information about the SQL server connection Veeam ONE uses to access its configuration database, resulting in remote code execution on the SQL server.
- CVE-2023-38548 - Allows an unprivileged user with access to the Veeam ONE Web Client to obtain the NTLM hash of the account used by the Veeam ONE Reporting Service.
- CVE-2023-38549 - Allows a user with the Veeam ONE Power User role to obtain the access token of a user with the Veeam ONE Administrator role.
- CVE-2023-41723 - permits a user with the Veeam ONE Read-Only User role to view the Dashboard Schedule.

Impact

- Elevation of Privilege
- Information Disclosure
- Remote Code Execution

Solution/ Workarounds

Apply fixes issued by the vendor:

- https://www.veeam.com/kb4508

Reference

https://thehackernews.com/2023/11/critical-flaws-discovered-in-veeam-one.html

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.