September 9, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Veeam published a security advisory to address vulnerabilities in the following products:

- Veeam Backup & Replication – 12.x version 12.1.2.172 and prior
- Veeam ONE – 12.x version 12.1.0.3208 and prior
- Veeam Service Provider Console – 8.x version 8.0.0.19552 and prior
- Veeam Agent for Linux – 6.x version 6.1.2.1781 and prior
- Veeam Backup for Nutanix AHV – 12.x version 12.5.1.8 and prior
- Veeam Backup for Oracle Linux Virtualization Manager – 12.x version 12.4.1.45 and prior
- Red Hat Virtualization – 12.x version 12.4.1.45 and prior

Technical Details

A deserialization of untrusted data vulnerability with a malicious payload can allow an unauthenticated remote code execution (RCE).

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-40709 CVE-2024-40710 CVE-2024-40711 CVE-2024-40712 CVE-2024-40713 CVE-2024-40714
- Veeam Security Advisory – kb4649
- Veeam Knowledge Base