June 12, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in Veeam Recovery Orchestrator (VRO). The vulnerability affects Veeam Recovery Orchestrator (VRO) version 7.0.0.337.

Technical Details

A vulnerability (CVE-2024-29855) in Veeam Recovery Orchestrator (VRO) version 7.0.0.337 may allow an attacker to access the VRO web UI with administrative privileges.

Note: The attacker must know the exact username and role of an account that has an active VRO UI access token to accomplish the hijack.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-29855
- Veeam Recovery Orchestrator Vulnerability (CVE-2024-29855)
- VRM Vulnerability Reports