September 10, 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 Progress published a security advisory to address vulnerabilities in multiple products. Included were critical updates for the following products:

- LoadMaster - version 7.2.60.0 and prior
- Multi-Tenant Hypervisor - version 7.1.35.11 and prior

Technical Details

We have not received any reports that this vulnerability has been exploited and we are not aware of any direct impact to customers. Nevertheless, we are encouraging all customers to upgrade their LoadMaster implementations as soon as possible to harden their environment. Make sure you are subscribed to announcement notifications via the Support Portal to receive timely notifications for important product updates.

This notification provides a brief description of the vulnerability and the related enhancements made in the affected releases.

Fix for CVE-2024-7591

It is possible for unauthenticated, remote attackers who have access to the management interface of LoadMaster to issue a carefully crafted http request that will allow arbitrary system commands to be executed. This vulnerability has been closed by sanitizing request user input to mitigate arbitrary system commands execution.

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

- Progress LoadMaster Security Vulnerability (CVE-2024-7591)