August 31, 2023

Overall rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a SAML token signature bypass vulnerability in VMware Tools. The vulnerability affects VMware Tools for Windows prior to 12.3.0 and VMware Tools for Linux 12.3.0. The VMware Tools 10.3.26 only applies to the older Linux releases.

Technical Details

VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor with man-in-the-middle (MITM) network positioning between vCenter server and the virtual machine may be able to bypass SAML token signature verification, to perform VMware Tools Guest Operations.

Exploitability Metrics
Attack Vector: Adjacent
Attack Complexity: High
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** 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.

References

- CVE-20223-20900
- VMSA-2023-0019

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: https://bcgov.sharepoint.com/sites/CITZ-ISB/SitePages/vulnerability-reports.aspx

If you have any questions, please reach out to OCIOSecurity@gov.bc.ca