

Overall Rating: High



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Ivanti published a security advisory to address vulnerabilities in the following product:

- Ivanti Endpoint Manager for Mobile (EPMM) – all versions

Technical Details

An insufficient authorization vulnerability in web component of EPMM prior to 12.1.0.1 allows an unauthorized attacker within the network to execute arbitrary commands on the underlying operating system of the appliance.

An insecure deserialization vulnerability in web component of EPMM prior to 12.1.0.1 allows an authenticated remote attacker to execute arbitrary commands on the underlying operating system of the appliance.

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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-36130 CVE-2024-36131 CVE-2024-36132 CVE-2024-34788
- [Security Advisory Ivanti Endpoint Manager for Mobile \(EPMM\) July 2024](#)
- [Ivanti Security Advisories](#)