

Overall Rating: High



This is a technical bulletin intended for technical audiences.

Summary

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

- HPE Athonet Mobile Core – versions 1.24.1.1 and prior and versions 1.23.4.2 and prior
- HPE Athonet IMS – versions 1.24.1.1 and prior

Technical Details

HPE Athonet Unauthenticated Remote Code Execution (RCE) vulnerability in OpenSSH's Server (RegreSSHion)

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-2024-6387
- [HPE Security Bulletin - hpesbnw04674en_us](#)
- [HPE Security Bulletin Library](#)