November 22, 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 HPE published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- HPE Edgeline e920, e920d and e920t Server Blades – firmware versions prior to 1.78_10-31-2023
- HP-UX OpenSSL Software – versions prior to A.01.01.01w.001

Technical Details

Potential security vulnerabilities have been identified in HPE Edgeline servers. These vulnerabilities could be locally exploited to allow escalation of privilege and/or information disclosure and/or denial of service.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update, Juniper Secure Analytics 7.5.0 UP7 IF02 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-2023-23583, CVE-2023-0464
- HPE Security Bulletin - hpesbhf04554en_us
- HPE Security Bulletin - hpesbux04564en_us
- HPE Security Bulletins

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: Cybersecurity Alerts