

Overall rating: Critical



This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that HPE published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- ArubaOS – multiple versions
- InstantOS – multiple versions
- HPE Synergy 480 Gen10 Plus Compute Module – versions prior to 1.90_10-19-2023
- HPE SimpliVity 380 Gen10 Plus – versions prior to OmniStack Firmware 2023_0913
- HPE ProLiant Server – multiple versions and platforms
- HPE Cray EX235n Server – versions prior to 1.3.1 (HFP 23.9)
- HPE Cray Compute Blade – multiple versions and platforms
- HPE StoreEasy Storage – multiple versions and platforms

Technical Details

Potential security vulnerabilities have been identified in Hewlett Packard Enterprise OneView and HPE OneView Global Dashboard (OVGD) Software. These vulnerabilities could be remotely exploited to allow authentication bypass.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify [VRM](#) with any questions or concerns you may have.

References

- CVE-2023-23583, CVE-2023-30908, CVE-2023-30909
- [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](#)