

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 multiple HPE products vulnerabilities. Included were updates for the following:

HPE SimpliVity 380 Gen10 – versions prior to OmniStack Firmware version 2023_0803

HPE SimpliVity 380 Gen10 G – versions prior to OmniStack Firmware version 2023_0803

HPE SimpliVity 380 Gen10 H – versions prior to OmniStack Firmware version 2023_0803

HPE SimpliVity 190r Gen10 Server – versions prior to OmniStack Firmware version 2023_0803

HPE SimpliVity 170r Gen10 Server – versions prior to OmniStack Firmware version 2023_0803

Aruba Virtual Intranet Access (VIA) Windows Client Only – version 4.5 and prior

Technical Details

- A vulnerability in the HPE Aruba Networking Virtual Intranet Access (VIA) client could allow local users to elevate privileges. Successful exploitation could allow execution of arbitrary code with NT AUTHORITY\SYSTEM privileges on the operating system.
- Local: Access Restriction Bypass, Bypass Security Restrictions, Denial of Service (DoS), Disclosure of Sensitive Information, memory corruption; Remote: Access Restriction Bypass, Bypass Security Restrictions, Code Execution, Denial of Service (DoS), Disclosure of Sensitive Information, memory corruption.

Exploitability Metrics

Attack Vector: Local

Attack Complexity: Low

Privileges Required: Low

User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software patch exists to address these 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

The Cyber Centre encourages users and administrators to review the provided web links and apply the necessary updates.

- [HPE Security Bulletin – hpesbnw04527en_us](#)
- [HPE Security Bulletin – hpesbhf04463en_us](#)
- [HPE Security Bulletins](#)
- CVE-2023-38401 CVE-2023-38402 CVE-2022-33894 CVE-2023-31432 CVE-2023-31926 CVE-2023-31427 CVE-2023-31425 CVE-2022-3786
- [HPE Security Bulletin Library](#)

Regards

Peter Kremer
Technical Analyst
Information Security Branch (ISB)
Office TEL 604 398 4741
Information Security Branch
Office of the Chief Information Officer
PO Box 9412 | Stn Prov Govt | Victoria BC V8W 9V1