

Overall Rating: Critical



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 product:

- HPE Virtual Tape Repository (VTR) – versions T0964V01 and T0964V01^AAA to AAJ

Technical Details

There's a flaw in lz4. An attacker who submits a crafted file to an application linked with lz4 may be able to trigger an integer overflow, leading to calling of memmove() on a negative size argument, causing an out-of-bounds write and/or a crash. The greatest impact of this flaw is to availability, with some potential impact to confidentiality and integrity as well.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

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-2012-0876 CVE-2021-3520 CVE-2022-43680 CVE-2023-52425 CVE-2023-52426 CVE-2024-28757](#)
- [HPE Security Bulletin - hpesbns04698en_us](#)
- [HPE Security Bulletin Library](#)