

**Overall rating: Critical**



**This is a technical bulletin intended for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team is aware that between September 25 and October 1, 2023, Dell first published security advisories to address vulnerabilities in multiple products. Please consult [Security Advisories and Notices](#) for current and updated vulnerability notices.

- Dell Avamar Data Store Gen5a – firmware versions prior to 2.18.1
- Dell Container Storage Modules – versions prior to 1.8
- Dell Metro Node VS5 – versions prior to 8.0.0, BIOS versions prior to 2.17.1, iDRAC versions prior to 6.10.30.20 and NIC versions prior to 21.5.9

## Technical Details

See link below for full details.

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

## 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

- [Security Advisories and Notices](#)
- CVE-2023-31925 , CVE-2023-31424 , CVE-2023-31423 , CVE-2023-4162, CVE-2023-4163 CVE-2023-3489.

***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](#)