

Overall Rating - High



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

Summary

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

- Cloud Tiering Appliance – versions prior to 13.1.0.2.35
- Cloud Tiering Appliance – versions prior to 13.2.0.2.26
- Disk Library for mainframe DLm2500 – versions prior to 5.5.0.4
- Disk Library for mainframe DLm8500 – versions prior to 5.5.0.4

Technical Details

The code that processes control channel messages sent to `named` calls certain functions recursively during packet parsing. Recursion depth is only limited by the maximum accepted packet size; depending on the environment, this may cause the packet-parsing code to run out of available stack memory, causing `named` to terminate unexpectedly. Since each incoming control channel message is fully parsed before its contents are authenticated, exploiting this flaw does not require the attacker to hold a valid RNDC key; only network access to the control channel's configured TCP port is necessary. This issue affects BIND 9 versions 9.2.0 through 9.16.43, 9.18.0 through 9.18.18, 9.19.0 through 9.19.16, 9.9.3-S1 through 9.16.43-S1, and 9.18.0-S1 through 9.18.18-S1.

These vulnerabilities are rated as an overall **High** 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-2023-4504, CVE-2023-34241, CVE-2023-32360, CVE-2023-40217, CVE-2023-41105, CVE-2023-45648, CVE-2023-44487, CVE-2023-42795, CVE-2023-42794, CVE-2023-41080
- [Dell Security Update - Cloud Tiering Appliance v13.1](#)
- [Dell Security Update - Cloud Tiering Appliance v13.2](#)
- [Dell Security Update - Disk Library for mainframe DLm2500](#)
- [Dell Security Update - Disk Library for mainframe DLm8500](#)

- [Security Advisories and Notices](#)