November 15, 2023

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 has published a security advisory to address vulnerabilities in the following product:

- Dell NetWorker Virtual Edition – multiple versions
- Dell Secure Connect Gateway – version 5.18.00.20

Technical Details

A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html .

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-2023-31122, CVE-2023-35945, CVE-2023-4733, CVE-2023-20900
- Dell Security Update - DSA-2023-413
- Dell Security Update - DSA-2023-056
- Security advisories and notices

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