July 10, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a recently released ServiceNow security advisories to address vulnerabilities in the following products:

- DC Now Platform

Technical Details

ServiceNow has addressed an input validation vulnerability that was identified in Vancouver and Washington DC Now Platform releases. This vulnerability could enable an unauthenticated user to remotely execute code within the context of the Now Platform. ServiceNow applied an update to hosted instances, and ServiceNow released the update to our partners and self-hosted customers. Listed below are the patches and hot fixes that address the vulnerability. If you have not done so already, we recommend applying security patches relevant to your instance as soon as possible.

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-2024-4879 CVE-2024-5217 CVE-2024-5178
- https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1644293
- https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154