June 24, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

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

- IBM Business Automation Workflow containers – version 23.0.2 to V23.0.2-IF004
- IBM Business Automation Workflow traditional – version 23.0.2
- IBM Cognos Analytics – version 12.0 to 12.0.2 and version 11.2.0 to 11.2.4 FP2
- IBM Db2 on Cloud Pak for Data – multiple versions
- IBM Db2 Warehouse on Cloud Pak for Data – multiple versions
- IBM i – versions 7.3, 7.4 and 7.5
- IBM Maximo Application Suite (IoT Component) – version 8.8.x and 8.7.x
- IBM Security SOAR – version 51.0.2.0 and prior
- IBM Storage Insights (Data Collector) – version 20240510-0638 and prior
- IBM Storage Protect for Space Management – version 8.1.0.0 to 8.1.21.0
- IBM Storage Scale System – version 6.1.0.0 to 6.1.2.9 and version 6.1.3.0 to 6.1.9.2
- IBM Storage Virtualize – versions 8.4, 8.5 and 8.6
- IBM Watson Assistant for IBM Cloud Pak for Data – version 4.0.0 to 4.8.5
- IBM Watson Explorer Analytical Components – multiple versions
- IBM Watson Explorer DAE Foundational Components – multiple versions
- IBM Watson Explorer Foundational Components – multiple versions
- IBM Watson Speech Services Cartridge for IBM Cloud Pak for Data – version 4.0.0 to 4.8.5

Technical Details

Due to the improper handling of batch files in child_process.spawn / child_process.spawnSync, a malicious command line argument can inject arbitrary commands and achieve code execution even if the shell option is not enabled. Impact: Thank you, to ryotak for reporting this vulnerability and thank you Ben Noordhuis for fixing it. Summary The Node.js project will release new versions of the 18.x, 20.x, 21.x releases lines on or shortly after, Tuesday, April 9, 2024 in order to address:

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

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-2023-52425 CVE-2024-37532 CVE-2024-27980 CVE-2024-27268 CVE-2024-25026 CVE-2024-22353 CVE-2024-24783 CVE-2023-26159
- IBM Security Bulletins