December 18, 2023

Overall rating: Critical

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

Summary

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

- IBM Automation Decision Services – version 23.0.1
- IBM Cloud Pak for Business Automation – multiple versions
- IBM Maximo Application Suite - multiple versions and platforms
- IBM Process Mining – versions 1.14.2, 1.14.2 IF001 and 1.14.1
- IBM Security Guardium – version 11.5
- IBM Spectrum Control – version 5.4
- IBM Tivoli Netcool Impact – version 7.1.0
- IBM Watson Machine Learning Accelerator on Cloud Pak for Data – multiple versions

Technical Details

Brix crypto-js could allow a remote attacker to obtain sensitive information, caused by the use of a weak cryptographic hash algorithm. By utilize cryptographic attack techniques, an attacker could exploit this vulnerability to obtain sensitive information and use this information to launch further attacks against the affected system.
CVSS Base score: 9.1

These vulnerabilities are rated as an overall **Critical** 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-2022-36392, CVE-2023-46233, CVE-2023-44981, CVE-2023-45133
- IBM Product Security Incident Response