December 4, 2023

Overall rating: Critical

BRITISH COLUMBIA

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 updates for the following:

- IBM Maximo Application Suite – Monitor Component – versions 8.10 and 8.11
- IBM Sterling B2B Integrator – multiple versions
- IBM Watson Speech Services Cartridge for IBM Cloud Pak for Data – version 4.0.0 to 4.7.4
- InfoSphere Information Server – version 11.7

Technical Details

System information could allow a remote attacker to execute arbitrary commands on the system, caused by a SSID command injection flaw in the WIFI Connections() and WIFI Networks() functions. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system.

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-2023-42810, CVE-2023-20863, CVE-2023-20860, CVE-2023-20861, CVE-2022-3697, CVE-2021-3583, CVE-2020-14330, CVE-2021-4041, CVE-2021-3701, CVE-2021-3702, CVE-2023-37920, CVE-2023-23931, CVE-2023-34969, CVE-2023-3899, CVE-2021-35942
- IBM Security Bulletin - IBM Maximo Application Suite - Monitor Component
- IBM Security Bulletin - IBM Sterling B2B Integrator
- IBM Security Bulletin - IBM Watson Speech Services Cartridge for IBM Cloud Pak for Data
- IBM Security Bulletin - InfoSphere Information Server

- IBM Product Security Incident Response