August 28, 2023

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

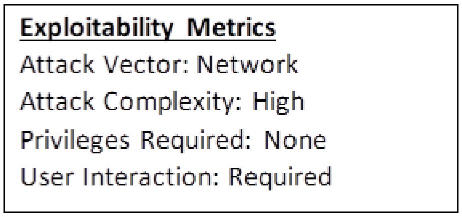
Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of IBM Security saw Node.js module vm2 is used internally by the Box and Snowflake connectors in Designer flows in IBM App Connect Enterprise Certified Container. IBM App Connect Enterprise Certified Container DesignerAuthoring, IntegrationServer and IntegrationRuntime operands that run Designer flows containing the Box or Snowflake nodes are vulnerable to arbitrary code execution.

CVE / Description / Product	Risk	CVSS
Node.js module vm2 is used internally by the Box and Snowflake connectors in Designer flows in IBM App Connect Enterprise Certified Container. IBM App Connect Enterprise Certified Container DesignerAuthoring. [CVE-2023-37466] **Product - App Connect Enterprise Certified Container**	**CRITICAL**	**9.8**
Node.js vm2 module could allow a remote attacker to execute arbitrary code on the system, caused by a flaw in the custom inspect function. [CVE-2023-37903] **Product – App Connect Enterprise Certified Container**	CRITICAL	9.8

Affected Products and Versions

Affected Product(s)	Version(s)
App Connect Enterprise Certified Container	4.1
App Connect Enterprise Certified Container	4.2
App Connect Enterprise Certified Container	5.0-lts
App Connect Enterprise Certified Container	5.1
App Connect Enterprise Certified Container	5.2
App Connect Enterprise Certified Container	6.0
App Connect Enterprise Certified Container	6.1
App Connect Enterprise Certified Container	6.2
App Connect Enterprise Certified Container	7.0
App Connect Enterprise Certified Container	7.1
App Connect Enterprise Certified Container	7.2
App Connect Enterprise Certified Container	8.0
App Connect Enterprise Certified Container	8.1
App Connect Enterprise Certified Container	8.2
App Connect Enterprise Certified Container	9.0



Exploitability Metrics

Attack Vector: Network

Attack Complexity: High

Privileges Required: None

User Interaction: Required

This vulnerability is rated as a Critical risk. A software patch 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.

References

- CVE-2023-37466 CVE-2023-37903
- Overview - Security Bulletins - IBM Support