مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in IBM Sterling Secure Proxy

Tracking #:432316767

Date:21-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in IBM Sterling Secure Proxy that could be exploited to execute malicious code, obtain confidential data, or disrupt service availability on affected systems.

TECHNICAL DETAILS:

IBM has disclosed multiple critical vulnerabilities affecting Sterling Secure Proxy (SSP), a crucial solution for secure data transfer across business networks. These vulnerabilities could allow attackers to inject commands, access sensitive information, or cause denial of service.

Critical Vulnerabilities:

- CVE-2024-41783 (CVSS 9.1)
  - Allows authenticated, privileged users to inject commands into the underlying operating system
  - Caused by improper validation of specific input types
- CVE-2024-38337 (CVSS 9.1)
  - Permits unauthorized attackers to retrieve or alter sensitive information
  - Stems from incorrect permission assignments

High-Severity Vulnerability:

- CVE-2024-25016 (CVSS 7.5)
  - Affects IBM MQ and IBM MQ Appliance 9.0, 9.1, 9.2, 9.3 LTS and 9.3 CD used by Sterling Secure Proxy
  - Allows remote unauthenticated attackers to launch denial of service attacks
  - Caused by incorrect buffering logic

Affected Product and Mitigations:

For CVE-2024-41783 and CVE-2024-38337:

Product	Affected Version(s)	Fixed-in Version(s)
IBM Sterling Secure Proxy	6.0.0.0 - 6.0.3.0	6.0.3.1 (fixpack) GA
IBM Sterling Secure Proxy	6.1.0.0	6.1.0.1 (fixpack) GA
IBM Sterling Secure Proxy	6.2.0.0	6.2.0.0 ifix 01

For CVE-2024-25016:

- Updates for IBM MQ and IBM MQ Appliance are available through IBM Fix Central

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by IBM.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.ibm.com/support/pages/node/7179166
- https://www.ibm.com/support/pages/node/7176189