مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-IBM Products

Tracking #:432316567

Date:27-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed IBM released patches addressing multiple vulnerabilities across several of its products.

TECHNICAL DETAILS:

IBM announced the release of critical patches addressing multiple vulnerabilities across several of its products. This includes two high-severity remote code execution (RCE) vulnerabilities in Data Virtualization Manager for z/OS and Security SOAR, which could potentially allow attackers to execute arbitrary code or cause denial-of-service (DoS) conditions.

Vulnerabilities Details:

1. **CVE-2024-52899 (Data Virtualization Manager for z/OS)**

- **Severity**: High (CVSS 8.5)
- **Impact**: This vulnerability allows a remote, authenticated attacker to inject malicious JDBC URL parameters, leading to arbitrary code execution on the server.
- **Affected Products**: Data Virtualization Manager for z/OS versions 1.1 and 1.2.
- **Fix**: IBM has released fix packs for the affected versions. Users are urged to follow the provided instructions in IBM's advisory to download and apply these fixes.

2. **CVE-2024-45801 (Security SOAR - Prototype Pollution)**

- **Severity**: High (CVSS 7.3)
- **Impact**: A prototype pollution flaw in the depth check of the DOMPurify component of the user interface can lead to remote code execution (RCE). By modifying the Object.prototype using malicious payloads, attackers could execute arbitrary code or cause a denial-of-service (DoS) condition.
- **Fix**: IBM Security SOAR version 51.0.4.0 removes the vulnerable DOMPurify component from the UI. Users should upgrade to this version following the provided instructions.

3. **CVE-2024-49353 (Watson Speech Services Cartridge for Cloud Pak for Data)**

- **Severity**: High
- **Impact**: This vulnerability can cause a crash of the Watson Speech Services Cartridge, potentially leading to a disruption of services.
- **Fix**: IBM has released patches to address this flaw. Users should apply the updates promptly to prevent service outages.

4. **CVE-2024-6119 (OpenSSL in Data Observability by Databand)**

- **Severity**: High (Denial-of-Service)
- **Impact**: A denial-of-service (DoS) vulnerability in OpenSSL used by Data Observability could lead to system instability or crashes under specific conditions.
- **Fix**: IBM has released patches for affected products. Immediate updating is recommended.

5. **Engineering Lifecycle Management Vulnerabilities**

- **Severity**: Medium and Low
- **Impact**: Several medium- and low-severity vulnerabilities were discovered in Engineering Lifecycle Management:
  - **Cross-site scripting (XSS)** vulnerabilities.
  - Ability to change dashboards across user sessions.
  - Exposure of plain text administrative passwords via network sniffing.
- **Fix**: These issues have been addressed in the latest updates. Users should follow the guidance for patching.

6. **Other Vulnerabilities**

- **IBM Workload Scheduler**: The scheduler was found to store user credentials in plain text.
- **Watson Query and Db2 Big SQL on Cloud Pak for Data**: Insufficient session expiration could allow attackers to access sensitive data if an authenticated session is still active.

RECOMMENDATIONS:

Install Patches and Apply Fixes for the affected products at the earliest

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/bulletin/