مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Sonatype Nexus Repository 2

Tracking #:432316525

Date:18-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Sonatype Nexus Repository 2, a widely-used repository manager for storing and distributing software artifacts. These vulnerabilities could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

1. **Remote Code Execution (RCE) - CVE-2024-5082**
    - Severity: High (CVSSv4 score: 7.1)
    - Impact: An attacker can execute arbitrary code by publishing a specially crafted Maven artifact
    - Risk: Complete system compromise upon artifact download.
2. **Stored Cross-Site Scripting (XSS) - CVE-2024-5083**
    - Severity: Medium (CVSSv4 score: 5.1)
    - Impact: Malicious scripts can be injected into Maven artifacts
    - Risk: Potential unauthorized actions or data theft when an administrator views the compromised artifact.

Affected Versions:

- All previous Sonatype Nexus Repository Manager 2.x OSS/Pro versions up to and including 2.15.1

Fixed Versions:

- Sonatype Nexus Repository Manager 2.x OSS/Pro version 2.15.2 or later

RECOMMENDATIONS:

- **Upgrade to Nexus Repository 2.15.2:** This version includes patches for both vulnerabilities.
- **Migrate to Nexus Repository 3:** For long-term security and enhanced features, consider migrating to the latest version of Nexus Repository 3.

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://support.sonatype.com/hc/en-us/articles/30694125380755-CVE-2024-5082-Nexus-Repository-2-Remote-Code-Execution
- https://support.sonatype.com/hc/en-us/articles/30693989411987-CVE-2024-5083-Nexus-Repository-2-Stored-XSS-Vulnerability