مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Sonatype Nexus Repository 3

Tracking #:432315907

Date:30-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High-Severity Vulnerability in Sonatype Nexus Repository 3 that could be exploited to gain unauthorized access to sensitive information on vulnerable systems.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2024-4956
- CVSS Score 7.5 High
- A path traversal vulnerability exists in Sonatype Nexus Repository 3. This vulnerability allows an unauthenticated attacker to craft a URL to download arbitrary files, including sensitive system files, from the underlying system.
- An attacker who successfully exploits this vulnerability could gain unauthorized access to sensitive information, including system configuration files, application source code, and other confidential data. This could potentially compromise the entire system and lead to a complete system takeover.
- Proof-of-concept (PoC) exploit code is publicly available

Affected Versions:

- All previous Sonatype Nexus Repository 3.x OSS/Pro versions up to and including 3.68.0

Mitigations:

- **Fixed Version:**
  - Sonatype Nexus Repository OSS/Pro version 3.68.1

- Additionally, Sonatype recommends rotating credentials for services connected to Nexus Repository or its host.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Sonatype.

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/29416509323923-CVE-2024-4956-Nexus-Repository-3-Path-Traversal-2024-05-16