مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical OpenStack Arbitrary File Access Vulnerability

Tracking #:432316026

Date:08-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability has been discovered in multiple core components of the OpenStack cloud infrastructure platform that could allow malicious actors to gain unauthorized access to sensitive data.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-32498-**The vulnerability exploits the QCOW2 image processing mechanism, allowing an authenticated user to supply a specially crafted QCOW2 image that references a specific data file path. When processed, the system could be tricked into returning the contents of the referenced file from the server, potentially leading to unauthorized access to sensitive data.
- This flaw could allow malicious actors to gain unauthorized access to sensitive data within Cinder (block storage), Glance (image management), and Nova (compute) services.

Affected versions:

- Cinder: Versions <22.1.3, >=23.0.0 <23.1.1, and 24.0.0
- Glance: Versions <26.0.1, 27.0.0, and >=28.0.0 <28.0.2
- Nova: Versions <27.3.1, >=28.0.0 <28.1.1, and >=29.0.0 <29.0.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest security updates released by OpenStack 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://security.openstack.org/ossa/OSSA-2024-001.html