Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical OpenStack Vulnerability Exposes Cloud Data

Date of Publication	Admiralty Code	TA Number
July 5, 2024	A1	TA2024261

Summary

First Seen: July 2, 2024
Affected Product: OpenStack
Impact: CVE-2024-32498 is a critical vulnerability in OpenStack's Cinder, Glance, and Nova components, allowing unauthorized file access through crafted QCOW2 images. This flaw can lead to exposure of sensitive data by manipulating image file paths. Patches have been released to address the issue, and applying these updates is essential to mitigate risks.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-32498	OpenStack Arbitrary File Access Vulnerability	OpenStack	✗	✗	✓

Vulnerability Details

#1

CVE-2024-32498 is a critical vulnerability affecting several components of the OpenStack, a widely cloud computing platform, specifically OpenStack Cinder up to version 24.0.0, Glance before version 28.0.2, and Nova before version 29.0.3. This issue allows arbitrary file access through the manipulation of QCOW2 images, which are commonly used for virtual machine disk images.

#2

This vulnerability arises from a flaw in how OpenStack validates image files containing references to other files. An attacker who has already gained access to the system can exploit this flaw to trick OpenStack services into reading or writing files on the host system. This bypasses security restrictions that normally isolate virtual machines from the underlying host, potentially leading to severe consequences.

#3

An attacker could leverage this vulnerability to execute malicious code directly on the host system, effectively taking complete control. They could also launch denial-of-service attacks, preventing legitimate users from accessing resources. Even more concerning, they might be able to steal sensitive information stored on the host, such as user data, system configurations, and even security credentials.

#4

This vulnerability affects all deployments of Cinder and Nova, while only Glance deployments with image conversion enabled are impacted. OpenStack users are advised to update to the latest versions immediately to mitigate the risk.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-32498	OpenStack Cinder: Versions up to 24.0.0. OpenStack Glance: Versions before 28.0.2. OpenStack Nova: Versions before 29.0.3.	cpe:2.3:a:openstack:cinder:*:*:*:*:*:*:*:* cpe:2.3:a:openstack:glance:*:*:*:*:*:*:*:* cpe:2.3:a:openstack:nova:*:*:*:*:*:*:*:*	CWE-20

Recommendations

Apply Security Patches: Ensure that you have applied the latest security patches provided by OpenStack. These patches address the vulnerability by preventing unauthorized access through manipulated QCOW2 images.

Monitor and Audit Logs: Regularly review access logs for any unusual activity that could indicate attempts to exploit this vulnerability. Implement real-time monitoring and alerting for suspicious actions related to image processing.

Implement Access Controls: Strengthen access controls to limit who can reference specific data file paths in QCOW2 images. Use role-based access control (RBAC) to ensure only authorized users can perform such actions.

Disable Image Conversion: If your deployment does not require image conversion, disable this feature in Glance. This can mitigate the risk in environments where image conversion is not necessary.

Isolate Image Processing: Run image processing tasks in isolated environments or containers to minimize the potential impact of an exploit. This containment strategy can prevent unauthorized access from spreading to other parts of the system.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA0002 Execution	TA0007 Discovery	TA0005 Defense Evasion
TA0040 Impact	TA0042 Resource Development	T1082 System Information Discovery	T1203 Exploitation for Client Execution
T1068 Exploitation for Privilege Escalation	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits
T1565 Data Manipulation	T1222 File and Directory Permissions Modification	T1190 Exploit Public-Facing Application	

Patch Link

https://security.openstack.org/ossa/OSSA-2024-001.html

References

https://securityonline.info/cve-2024-32498-critical-openstack-flaw-exposes-cloud-data-to-attackers/

https://access.redhat.com/security/cve/CVE-2024-32498

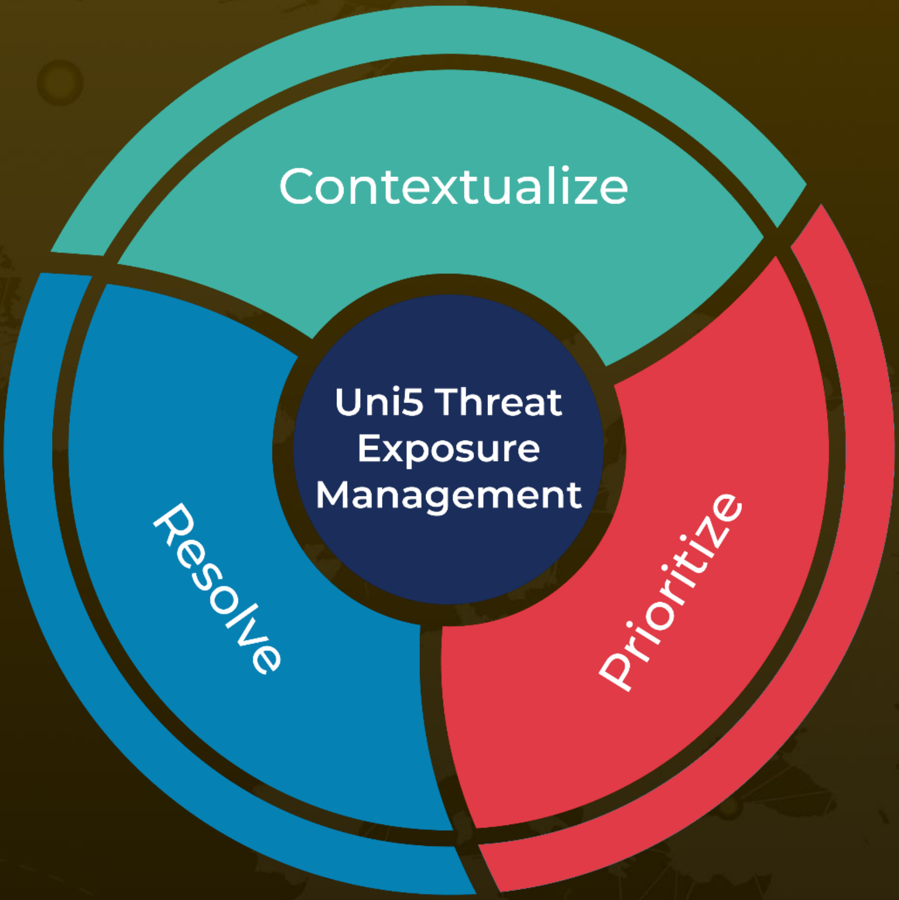
https://www.openwall.com/lists/oss-security/2024/07/02/2

https://bugs.launchpad.net/nova/+bug/2059809

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 5, 2024 • 6:30 AM

More at www.hivepro.com