Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

OpenMetadata Flaws Exploited for Cryptojacking on Kubernetes

Date of Publication	Admiralty Code	TA Number
April 19, 2024	A1	TA2024155

Summary

First Seen: March 15, 2024
Affected Platform: OpenMetadata
Impact: Threat actors are exploiting new vulnerabilities in OpenMetadata to hijack Kubernetes workloads for cryptomining. These vulnerabilities allow attackers to bypass security and remotely control systems running OpenMetadata versions before 1.3.1. Upgrading to version 1.3.1 or later is essential to protect your Kubernetes environments.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-28255	OpenMetadata Improper Authentication Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-28847	OpenMetadata Code Injection Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-28253	OpenMetadata Code Injection Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-28848	OpenMetadata Code Injection Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-28254	OpenMetadata OS Command Injection Vulnerability	OpenMetadata	✗	✗	✓

Vulnerability Details

#1

Threat actors are exploiting critical vulnerability in OpenMetadata that allows attackers to gain access to Kubernetes workloads and leverage them for cryptomining activity. Attackers exploit these vulnerabilities by identifying and targeting Kubernetes workloads of OpenMetadata exposed to the internet. Once a vulnerable version is identified, attackers exploit the vulnerabilities to bypass authentication and gain remote code execution on the container running the vulnerable OpenMetadata image.

#2

After gaining initial access, attackers use a series of reconnaissance commands to gather information about the victim environment. They then download a cryptomining-related malware from a remote server. The attackers then initiate a reverse shell connection to their remote server using Netcat tool, allowing them to remotely access the container and gain better control over the system.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-28255	OpenMetadata versions prior to 1.2.4	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	CWE-287
CVE-2024-28847	OpenMetadata versions prior to 1.2.4	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	CWE-94
CVE-2024-28253	OpenMetadata versions prior to 1.3.1	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	CWE-94
CVE-2024-28848	OpenMetadata versions prior to 1.2.4	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	CWE-94

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-28254	OpenMetadata versions prior to 1.2.4	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Update OpenMetadata: Ensure that OpenMetadata is updated to the latest version (1.3.1 or later) to patch known vulnerabilities. Regularly monitor for updates and apply patches promptly.

Implement Strong Authentication: Enforce strong authentication mechanisms for accessing OpenMetadata and other Kubernetes workloads. Avoid using default credentials and consider implementing multi-factor authentication where possible.

Network Segmentation: Implement network segmentation to restrict access to Kubernetes workloads, minimizing exposure to potential attackers. Use firewalls and network policies to control traffic flow between different components of the Kubernetes environment.

Vulnerability Scanning: Conduct regular vulnerability scans of Kubernetes clusters to identify and address any security weaknesses or misconfigurations. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0043 Reconnaissance	TA0002 Execution
TA0007 Discovery	TA0042 Resource Development	TA0008 Lateral Movement	TA0040 Impact

TA0011 Command and Control	TA0004 Privilege Escalation	TA0005 Defense Evasion	T1190 Exploit Public-Facing Application
T1496 Resource Hijacking	T1059 Command and Scripting Interpreter	T1021 Remote Services	T1590 Gather Victim Network Information
T1082 System Information Discovery	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1588 Obtain Capabilities
T1070 Indicator Removal	T1588.006 Vulnerabilities	T1588.005 Exploits	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7c6f0bae1e588821bd5d66cd98f52b7005e054279748c2c851647097fa2ae2df, 19a63bd5d18f955c0de550f072534aa7a6a6cc6b78a24fea4cc6ce23011ea01d, 31cd1651752eae014c7ceaaf107f0bf8323b682ff5b24c683a683fdac7525bad
IPv4	8[.]222[.]144[.]60, 61[.]160[.]194[.]160, 8[.]130[.]115[.]208

Patch Details

Upgrade OpenMetadata to version 1.3.1 or later

Link:
https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-6wx7-qw5p-wh84

https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-8p5r-6mvv-2435

https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-7vf4-x5m2-r6gr

https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-5xv3-fm7g-865r

https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-j86m-rrpr-g8gw

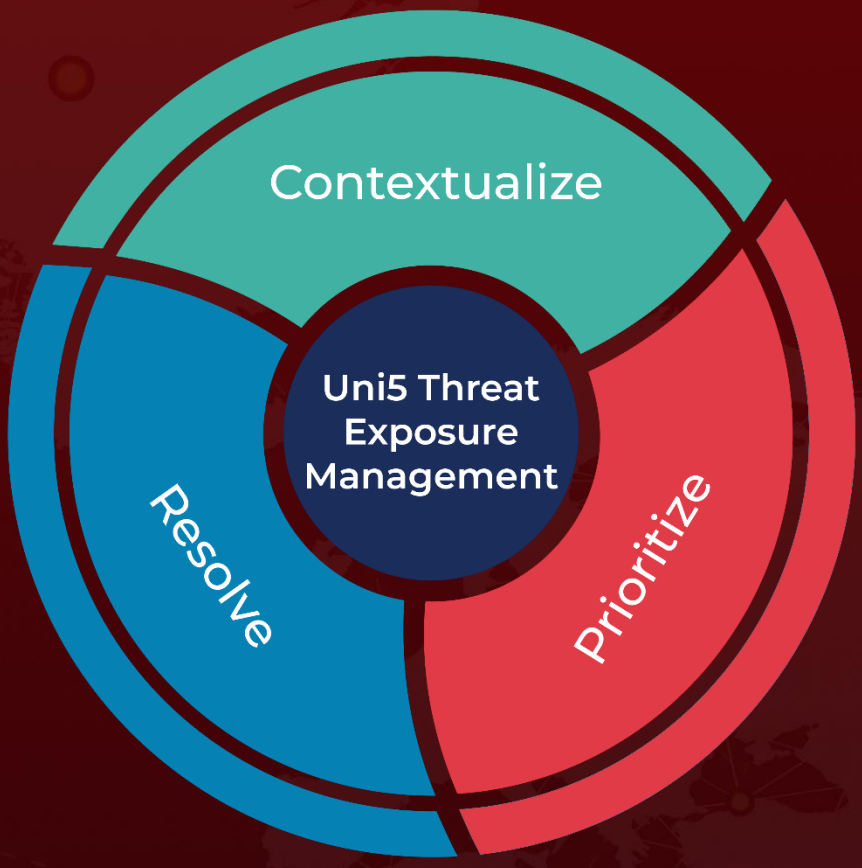
References

https://www.microsoft.com/en-us/security/blog/2024/04/17/attackers-exploiting-new-critical-openmetadata-vulnerabilities-on-kubernetes-clusters/

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

April 19, 2024 • 4:45 AM

More at www.hivepro.com