

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

POC Exploit Code Released for Apache HugeGraph RCE Vulnerability

Date of Publication

June 10, 2024

Admiralty Code

A1

TA Number

TA2024223




Summary

First Seen: April 22, 2024

Affected Product: Apache HugeGraph-Server

Impact: CVE-2024-27348 is a critical RCE vulnerability in Apache HugeGraph-Server versions before 1.3.0. It allows attackers to remotely execute code by sending malicious Gremlin commands. Upgrading to version 1.3.0 and enabling authentication are recommended to mitigate this risk.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-27348	Apache HugeGraph-Server Remote Command Execution Vulnerability	Apache HugeGraph-Server			

Vulnerability Details

#1

CVE-2024-27348 is a critical remote code execution (RCE) vulnerability in Apache HugeGraph, a popular graph database. This flaw affects versions 1.0.0 to 1.2.1 when running on Java 8 or Java 11. The vulnerability stems from the Gremlin traversal language interface, which can be exploited by sending specially crafted requests to the Gremlin server. This can allow an attacker to execute arbitrary code on the underlying system, leading to unauthorized access, data manipulation, and potential system compromise.

#2

HugeGraph is a powerful, open-source graph database developed by Baidu to manage large-scale graph data and complex queries with high performance. It supports various data models and query languages, including Gremlin, Cypher, and SPARQL, offering flexible and efficient data management.

#3

The vulnerability is due to insufficient filtering of reflections in the SecurityManager, allowing attackers to bypass security checks. The patch addresses this by filtering critical system classes and adding new security checks.

#4

The vulnerability has been assigned a CVSS score of 9.8, indicating its high severity. To mitigate potential security threats, users are advised to update to the latest version of Apache HugeGraph-Server, as proof-of-concept (PoC) exploit for the vulnerability has been released.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-27348	Apache HugeGraph-Server from version 1.0.0 to before 1.3.0 in Java8 & Java11	cpe:2.3:a:apache:hugegraph-server:*:*:*:*:*	CWE-77

Recommendations



Apply Patch: The most effective mitigation is to update Apache HugeGraph Server to version 1.3.0 or newer, where the vulnerability has been patched. Regularly check for updates and apply them promptly to ensure that your system is protected against known vulnerabilities.



Network Configuration: Restrict access to the server by configuring the "Whitelist-IP/port" function to limit access only to trusted IP addresses and ports. This minimizes the exposure to potential attacker.



Monitor Activity: Closely monitor your Apache HugeGraph Server instances for any suspicious activity that might indicate exploitation attempts.



Enable User Authentication: By default, HugeGraph does not enable user authentication. To enable it, modify the configuration file (hugegraph.properties) to set auth.enable=true. Ensure you are using the Java 11 version as it is recommended for enhanced security.



Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>T1059</u> Command and Scripting Interpreter
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1190</u> Exploit Public-Facing Application
<u>T1068</u> Exploitation for Privilege Escalation			

Patch Details

Upgrade Apache HugeGraph-Server to version 1.3.0 with Java11 & enable the Auth system

Links:

<https://hugegraph.apache.org/docs/download/download/>

<https://hugegraph.apache.org/docs/changelog/hugegraph-1.3.0-release-notes/>

References

<https://lists.apache.org/thread/nx6g6htyhpgtzsocybm242781o8w5kq9>

<https://blog.securelayer7.net/remote-code-execution-in-apache-hugegraph/>

<https://github.com/Zeyad-Azima/CVE-2024-27348>

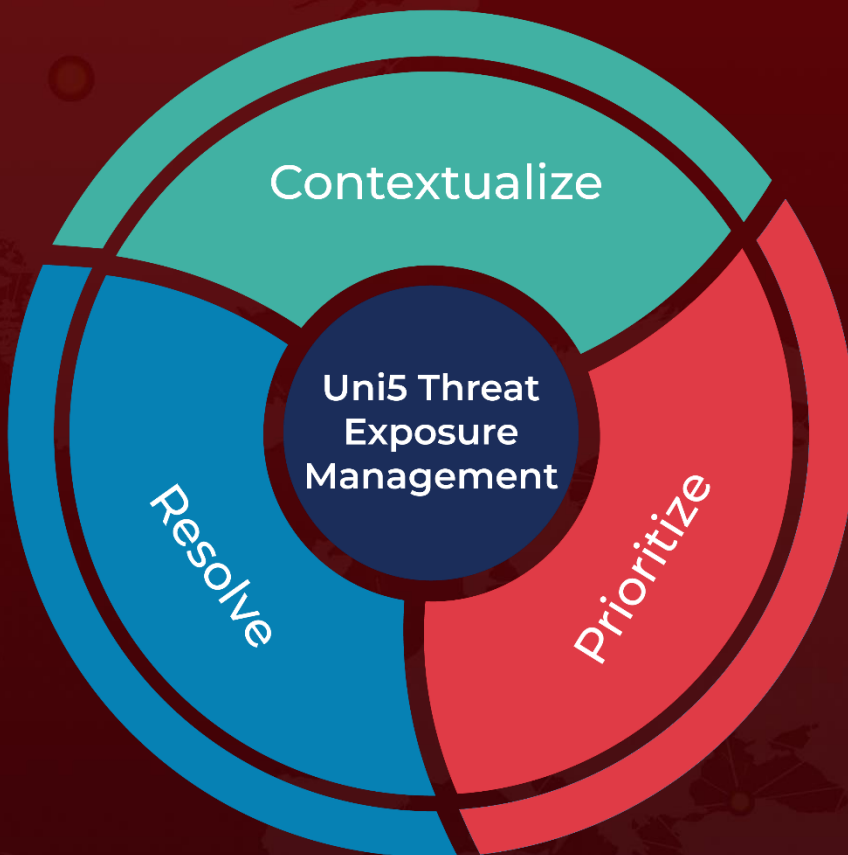
<https://github.com/advisories/GHSA-29rc-vq7f-x335>

<https://github.com/kljunowsky/CVE-2024-27348>

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

June 10, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com