Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Apache Avro Flaw Opens Door to Remote Code Execution

Date of Publication

October 8, 2024

Admiralty Code

A1

TA Number

TA2024383

Summary

First Seen: October 3, 2024
Affected Products: Apache Avro Java SDK
Impact: A critical security vulnerability, designated as CVE-2024-47561, has been discovered in the Apache Avro Java Software Development Kit (SDK). This flaw poses a serious threat, as it allows attackers to execute arbitrary code on vulnerable systems. Organizations that rely on Apache Avro for data serialization and processing face substantial risks, including potential system compromise and unauthorized access. The exploitation of this vulnerability requires no user interaction and can be carried out without any privileges, underscoring the urgency for users to apply security patches immediately to safeguard against potential attacks.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-47561	Apache Avro Java SDK Arbitrary Code Execution Vulnerability	Apache Avro Java SDK	✗	✗	✓

Vulnerability Details

#1 A critical vulnerability has been identified in the Apache Avro Java Software Development Kit (SDK), tracked as CVE-2024-47561. This flaw affects all versions prior to 1.11.4 and poses a significant risk of arbitrary code execution, potentially compromising the entire system. Apache Avro is a widely-used data serialization system designed to efficiently handle large volumes of data in distributed systems like Apache Hadoop, Kafka, and Spark. The Apache Avro Java SDK provides essential support by defining a binary format that enables data to be serialized and deserialized across different platforms in a compact and efficient manner.

#2 The vulnerability resides in the schema parsing functionality of the SDK, specifically in versions 1.11.3 and earlier. This weakness allows threat actors to exploit the flaw and execute arbitrary code on affected systems, granting them control and significantly increasing the risk of complete system compromise.

#3 Users of versions prior to 1.11.4 must take immediate action to upgrade to the latest version to safeguard their systems. Proactive patching and vigilant monitoring are crucial to protecting against high-severity vulnerabilities like this one and ensuring the integrity of your data and systems.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-47561	Apache Avro Java SDK before 1.11.4	cpe:2.3:a:apache:avro:*:*:*:*:*:*:*:*	CWE-502

Recommendations

Upgrade Immediately: Upgrade the Apache Avro Java SDK to version 1.11.4 or 1.12.0. These versions include critical security fixes that address known vulnerabilities. Ensure that all systems utilizing Apache Avro are updated to one of these versions to prevent potential exploitation.

Isolate if Upgrade is Not Possible: If immediate upgrading is not feasible, isolate any systems running older, vulnerable versions of Apache Avro from untrusted networks. Limit external access and restrict communication to only trusted internal networks to reduce exposure to potential attacks.

Avoid Parsing User-Provided Schemas: Refrain from directly parsing schemas submitted by users. Malicious actors may craft specially designed schemas to exploit vulnerabilities, leading to potential system compromise.

Sanitize Schemas Before Parsing: If it is necessary to handle user-provided schemas, ensure that they are thoroughly sanitized before any parsing occurs. Remove any potentially harmful or malformed elements from the schema to prevent malicious data from being processed. This step is crucial in preventing schema-based attacks.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation
T1190 Exploit Public-Facing Application			

Patch Details

Users are advised to upgrade to version 1.11.4 or 1.12.0, which address and resolve this issue effectively.

Links: https://avro.apache.org/blog/2024/08/05/avro-1.12.0/

https://avro.apache.org/blog/2024/09/22/avro-1.11.4/

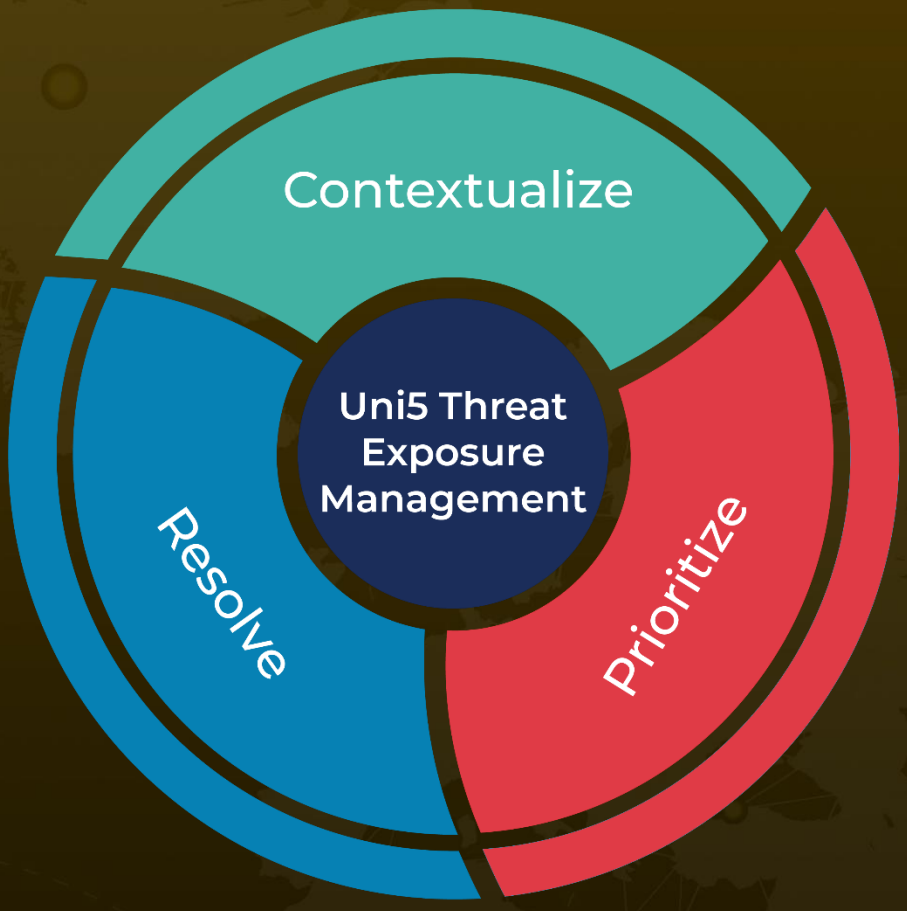
References

https://lists.apache.org/thread/c2v7mhqnmq0jmbwxqq3r5jbj1xg43h5x

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

October 8, 2024 . 6:30 PM

More at www.hivepro.com