Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Apache MINA Flaw Exposes Systems to Remote Code Execution

Date of Publication	Admiralty Code	TA Number
December 30, 2024	A1	TA2024477

Summary

First Seen: December 2024
Affected Products: Apache MINA
Impact: The Apache Software Foundation (ASF) has released essential patches to fix a critical vulnerability in the MINA Java network application framework. Designated as CVE-2024-52046, this flaw could enable remote code execution under certain conditions, affecting multiple versions of the widely adopted networking library and raising serious security concerns.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-52046	Apache MINA Remote Code Execution Vulnerability	Apache MINA	✗	✗	✓

Vulnerability Details

#1

A critical vulnerability, tracked as CVE-2024-52046, has been discovered in Apache MINA, a widely used Java networking library. This flaw could enable attackers to execute remote code by exploiting insecure deserialization processes, making it a significant security concern for organizations using the affected versions. In response, the Apache Software Foundation (ASF) has released essential patches to address this maximum-severity issue.

#2 The vulnerability resides in the ObjectSerializationDecoder component of Apache MINA, which utilizes Java's native deserialization protocol to process serialized data. However, the decoder lacks robust security checks, leaving it vulnerable to exploitation. Attackers can craft and send malicious serialized data to manipulate the deserialization process, potentially leading to remote code execution (RCE) attacks.

#3 This issue specifically impacts applications that invoke the IoBuffer#getObject() method, especially when a ProtocolCodecFilter instance using the ObjectSerializationCodecFactory class is included in the filter chain. To mitigate this risk, the updated Apache MINA framework introduces stricter controls for deserialization. Developers must now explicitly specify which classes are allowed for deserialization using one of the new methods in the ObjectSerializationDecoder. Simply upgrading the framework will not fully resolve the issue.

#4 It is worth noting that the FtpServer, SSHd, and Vysper sub-projects are not affected by this vulnerability. Organizations using Apache MINA must act promptly to mitigate the associated risks. The Apache MINA team has released updates that address this issue by enhancing the security of the deserialization process, including stricter validation of incoming serialized data.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-52046	Apache MINA 2.0 through 2.0.26, Apache MINA 2.1 through 2.1.9, Apache MINA 2.2 through 2.2.3	cpe:2.3:o:apache:mina:*:*:*:*:*:*:*	CWE-94

Recommendations

Apply Patches: Upgrade to the latest patched version of Apache MINA 2.0.27, 2.1.10, or 2.2.4 immediately. Ensure the update incorporates the newly implemented deserialization safeguards.

Restrict Deserialization: Configure the ObjectSerializationDecoder to explicitly allow only safe, validated classes for deserialization. Use the provided methods for class name matching, pattern-based acceptance, or wildcard specifications to ensure robust controls.

Isolate Vulnerable Systems: If immediate patching is not feasible, consider isolating systems running vulnerable versions of Apache MINA to reduce the attack surface.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1059 Command and Scripting Interpreter			

Patch Details

Update to the patched versions of Apache MINA (2.0.27, 2.1.10, or 2.2.4) without delay. Postponing updates significantly heightens the risk of exploitation and potential system compromise.

Link: https://mina.apache.org/downloads-mina_2_0.html

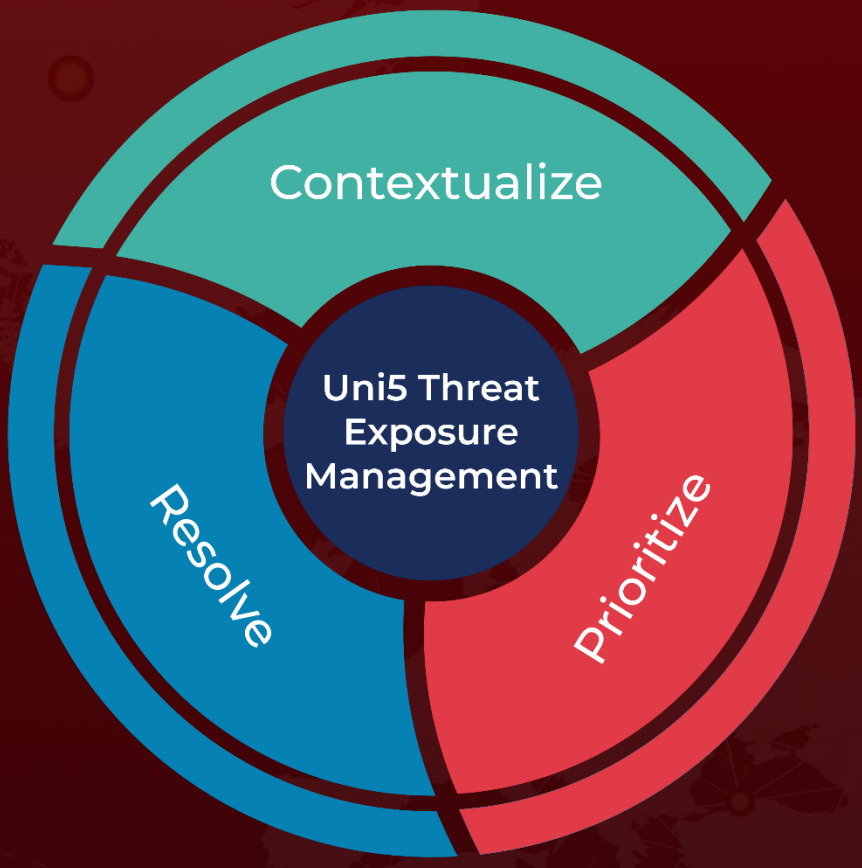
References

https://lists.apache.org/thread/4wxktgjpggdbto15d515wdctohb0qmv8

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

December 30, 2024 • 6:15 AM

More at www.hivepro.com