

Hiveforce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **A Deserialization Vulnerability Found in Apache Dubbo**

Date of Publication

March 22, 2023

Admiralty Code

A1

TA Number

TA2023154



# Summary

**First Seen:** March 08, 2023

**Affected Product:** Apache Dubbo

**Impact:** The vulnerability that allows remote attackers to execute arbitrary code on the target system.

## CVEs

CVE	NAME	PATCH	CISA KEV
CVE-2023-23638	Apache Dubbo Deserialization Vulnerability		

# Vulnerability Details

Apache has released a security notice for a deserialization vulnerability (CVE-2023-23638) in Apache Dubbo that allows remote attackers to execute arbitrary code on the target system. Versions affected are Apache Dubbo 2.7.x <= 2.7.21, Apache Dubbo 3.0.x <= 3.0.13, and Apache Dubbo 3.1.x <= 3.1.5. Users are advised to update to the latest version and close the Dubbo server port open to the public network or only allow trusted IP access.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-23638	Apache Dubbo: 3.0.x <= 3.0.13, 3.1.x <= 3.1.5, 2.7.x <= 2.7.21	cpe:2.3:a:apache:dubbo:*:*:*:*:*	CWE-502

# Recommendations



## Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.



## Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

## Potential MITRE ATT&CK TTPs

<b>TA0042</b> Resource Development	<b>TA0001</b> Initial Access	<b>TA0002</b> Execution	<b>T1588</b> Obtain Capabilities
<b>T1588.006</b> Vulnerabilities	<b>T1203</b> Exploitation for Client Execution	<b>T1190</b> Exploit Public-Facing Application	



## Patch Link

<https://github.com/apache/dubbo/releases>



## References

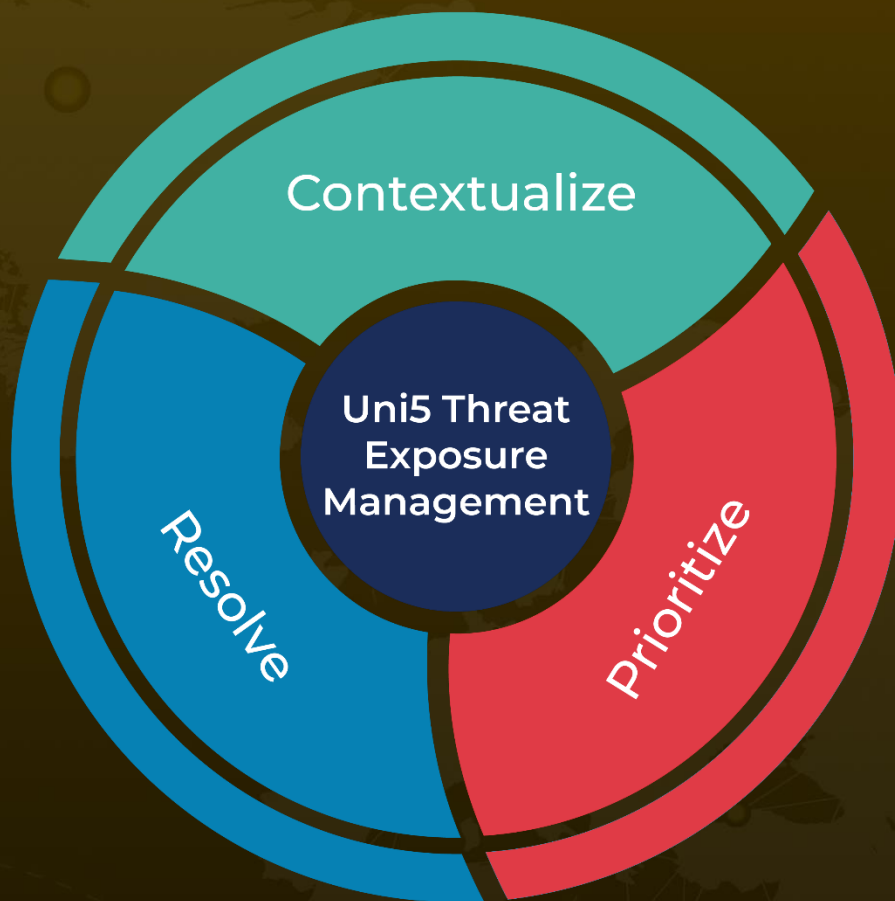
<https://nsfocusglobal.com/apache-dubbo-deserialization-vulnerability-notice-cve-2023-23638/>

<https://www.cisa.gov/news-events/bulletins/sb23-072>

# 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

**March 22, 2023 • 11:30 PM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)