PUBLIC - FOR EXTERNAL USE: (TLP: WHITE)

Security Advisory Report - OBSO-2401-02

Apache ActiveMQ OpenWire Protocol Class Type Manipulation Arbitrary Code Execution Vulnerability (CVE-2023-46604)

Status:	General Release
Release Date:	2024-01-10 14:27:48
Last Update:	2024-01-10 14:32:00
Version:	1.0

Summary

Apache ActiveMQ is vulnerable to Remote Code Execution. The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath.

The vulnerability affects Atos Unify OpenScape UC and Atos Unify Common Management Platform. If configured properly the ActiveMQ port is not exposed to the Internet.

The severity is rated critical to high.

Details

The vulnerability is rated criical to high with a CVSS 3.1 Base score of 8.8 (high).
CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

This vulnerability has been included into CISA Known Exploited Vulnerabilities catalogue. Public exploits are available.

Affected Products

Product statements are related only to supported product versions. Products which have reached End of

Support (M44) status are not considered.

Products confirmed affected

OpenScape UC V10 before V10 R5.8.0 (available)
OpenScape Common Management Platform V10 before V10 R5.8.0 (available)

Recommended Actions

Customers are advised to:

- Update the systems with the available fix releases.
- Check the configuration and implement the recommended security configuration measures.

Recommended security configuration measures:

- Implement the recommended security configuration measures of the OpenScape UC Application V10 Security Checklist [1].
- Ensure that all server components of the OpenScape UC solution are operated in a secured subnet that is protected by an external firewall. Only expose port 61616 for the required communication with the Façade Server.
- For UC push notifications restrict access outbound from UC Frontend/UC Backend to the Façade Server on port 61616.
- Do not allow inbound access from Façade Server to UC Frontend/Backend on port 61616 (inbound access is not required).

References

- [1] OpenScape UC Application V10 Security Checklist
- NVD CVE-2023-46604
- https://activemq.apache.org/security-advisories.data/CVE-2023-46604
- https://issues.apache.org/jira/browse/AMQ-9370
- https://github.com/X1r0z/ActiveMQ-RCE
- https://inthewild.io/vuln/CVE-2023-46604
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/bulletins/sb23-303
- https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-283657-1032.html
- https://thehackernews.com/2023/11/hellokitty-ransomware-group-exploiting.html
- https://thehackernews.com/2023/11/new-poc-exploit-for-apache-activemq.html

Version Change History

Version	Date	Description
1.0	10.01.2024	- Initial release

Security Advisories are released as part of Mitel Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product, and service names are trademarks or registered trademarks of their respective holders.