NCSC

National Cyber Security Centre

2311020004-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Apache ActiveMQ RCE Vulnerability - CVE-2023-46604

Thursday 2nd November, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Apache ActiveMQ has released a security advisory that addresses the critical vulnerability CVE-2023-46604. CVE-2023-46604 poses a significant risk to affected organisations, as exploitation may allow an attacker to achieve remote code execution (RCE) on vulnerable Apache ActiveMQ instances.

You can view the Apache ActiveMQ advisory here.

Products Affected

Apache ActiveMQ is an open-source message broker software that implements the Java Message Service (JMS) API. It is widely used in enterprise and web applications to facilitate communication between various software components.

Affected versions:

- Apache ActiveMQ 5.18.0 before 5.18.3
- Apache ActiveMQ 5.17.0 before 5.17.6
- Apache ActiveMQ 5.16.0 before 5.16.7
- Apache ActiveMQ before 5.15.16
- Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3
- Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6
- Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7
- Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16

Impact

Successful exploitation of this vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands. This could lead to complete system compromise.

Recommendations

The NCSC strongly advises organisations to identify any assets that are running affected Apache ActiveMQ versions and to upgrade these to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3, which fixes this issue.

Please see this advisory from Rapid7 with details of active exploitation, a POC and IOCs.

Further information can be found here:

- Apache ActiveMQ Security Advisory: CVE-2023-46604
- Apache ActiveMQ Security Tags
- CVE-2023-46604 Proof of Concept
- Openwall Security Advisory: CVE-2023-46604
- Rapid7 Security Advisory: CVE-2023-46604
- Rapid7 Technical Analysis: CVE-2023-46604

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie