Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

TLP:WHITE

Advisory 2021-004: Active exploitation of ForgeRock Access Manager / OpenAM servers

Summary

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has identified targeting and compromise of Australian organisations with vulnerable internet-accessible servers running ForgeRock Access Manager (ForgeRock AM). ForgeRock AM was previously known as OpenAM. The ACSC has observed malicious actors exploiting the vulnerability in ForgeRock AM/OpenAM to gain initial access to networks in multiple organisations, and facilitate further access within these networks. On 7 July 2021 the ACSC alerted organisations that this vulnerability was being actively exploited[1]. This ACSC advisory provides recommendations for securing ForgeRock AM against vulnerability CVE-2021-35464, and advice on identifying potential successful exploitation of this vulnerability.

Vulnerability details

On 23 June 2021, CVE-2021-35464 was raised in relation to ForgeRock Access Manager (ForgeRock AM), an identity and access management solution.

When exploited, the vulnerability allows Remote Code Execution (RCE) on the server through unsafe Java deserialisation in the Jato framework, which is used by both ForgeRock AM and the open-source OpenAM.

Affected Versions

For the most up to date information, please refer to ForgeRock security advisory #202104[2]. As of 9 July 2021, known vulnerable versions of ForgeRock AM include:

- AM 6.5.3
- AM 6.5.2.x
- AM 6.5.1
- AM 6.5.0.x
- AM 6.0.0.x
- Any version prior to 6

The ACSC understands this vulnerability may also affect other forks of OpenAM, specifically versions using Java 8 or earlier.

Mitigation and detection

Recommended prioritised mitigations

The ACSC recommends immediately updating all vulnerable ForgeRock AM instances to the latest version (version 7 or above). There is no patch available as the vulnerability is not present in newer versions of the software, however

[1] ACSC alert - https://www.cyber.gov.au/acsc/view-all-content/alerts/forgerock-open-am-critical-vulnerability

[2] ForgeRock Security Advisory #202104 - https://backstage.forgerock.com/knowledge/kb/article/a47894244

ForgeRock provided a workaround for this vulnerability on 29 June 2021, detailed in ForgeRock security advisory #202104.

If updating ForgeRock AM is not immediately possible, the ACSC recommends taking one of the following actions as soon as possible:

- Implement the workaround provided in ForgeRock security advisory #202104
- Prevent internet access to servers running vulnerable versions of ForgeRock AM
- Shut down servers running vulnerable versions of ForgeRock AM

These are temporary measures and only recommended where immediately updating is not possible.

Once updating to the latest version of ForgeRock AM or workaround measures have been applied, the ACSC strongly recommends organisations investigate all servers running vulnerable versions of ForgeRock AM for signs of compromise.

Recommended investigative actions

Regardless of when mitigations are applied, there remains a significant risk that malicious actors may have exploited and compromised servers running vulnerable versions of ForgeRock AM prior to these mitigations being applied. The ACSC has observed follow on activity from exploitation of this vulnerability including attempted lateral movement using native Linux functions and deployment of additional tools.

The following is a list of recommended investigative actions to check for signs of exploitation and compromise relating to this vulnerability. This guidance covers looking for evidence of exploitation of the ForgeRock AM vulnerability and initial post-exploitation activity. This list is not intended as complete investigative guidance for all stages of an intrusion.

- *Review HTTP and audit logs for evidence of exploitation*
    - Evidence of attempted exploitation can be seen in the httpd access logs, and can be identified by the following:
        - GET requests to the *openam/ccversion* resource, with the query of *Version?jato.pageSession=<serialised object>*
            - The complete entry will appear as: "*GET /openam/ccversion/Version?jato.pageSession=XXXXXXXXXXX*"
        - The serialised object is a Java serialised object, prepended with a null byte and base64 encoded. Base64 decoding the entire serialised object can reveal the commands that an actor was attempting to execute which informs further investigation.
        - Evidence of executed commands may be present in audit logs. These events can be correlated with the time of attempted exploitation to confirm whether or not the exploit was successful. The absence of entries does not guarantee a lack of exploitation.
- *Investigate security logs for evidence of lateral movement and further malicious access*
    - The ACSC has observed evidence of attempted lateral movement using ssh following exploitation. Investigation of relevant security logging in the time period following attempted exploitation may reveal evidence of lateral movement from affected servers to other hosts in the network through use of ssh.
- *Investigate creation of suspicious files following attempted exploitation*
    - Web shells and additional tools have been deployed following exploitation of victims. Organisations should review exposed servers running ForgeRock AM for evidence of files created following attempted exploitation.
    - A list of indicators of compromise seen to date is detailed in the Indicators of Compromise section below.

- The absence of any of these indicators is not a guarantee that exploitation and compromise has not occurred.

Indicators of Compromise

The ACSC has identified the following indicators of compromise from ongoing investigations, and recommends organisations search for presence of these indicators. Additionally, yara and STIX packages are available for download from cyber.gov.au to assist with detecting these files.

Indicator	Indicator Type	MITRE ATT&CK	Description	Version added
401.jsp	File name	T1505.003[3]	Web shell providing arbitrary command execution capability.	1
cmd.jsp 404.jsp	File name	T1505.003	jsp web shell providing command execution and file upload capability. Based on https://github.com/SecurityRiskAdvisors/cmd.jsp	1
reg.jsp	File name	T1505.003	Tool used to tunnel or bounce traffic elsewhere in a network. Originated from https://github.com/L-codes/Neo-reGeorg	1
a.zip b b.py e.c e.pl e.sh e.txt	File name	T1505.003	Alternate filenames seen in use by the actor.	1

[3] MITRE ATT&CK – Web Shell https://attack.mitre.org/techniques/T1505/003/

/home/openwis/apache-tomcat-7.0.59/webapps/openam/css/ /home/openwis/.j/ /opt/forgerock/openam/apache-tomcat/9.0.24/webapps/sso/css/ ../webapps/ipdiscovery/com_sun_web_ui/css/	Paths	Paths known to be used by the actor to download code or stage data for exfiltration.	1

Incident reporting

The ACSC is monitoring the situation and is able to provide assistance and advice as required. Organisations that have been impacted or require assistance can contact the ACSC via **1300 CYBER 1** (1300 292 371).

Traffic light protocol

Alert classification	Restriction on access and use
Red	**Highly restricted** **Access to and use by your Australian Cyber Security Centre (ACSC) contact officer(s) only.** You must ensure that your ACSC contact officer(s) does not disseminate or discuss Red alerts with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ACSC contact officer(s).
Amber	**Restricted internal access and use only.** Subject to the below, you shall only make Amber alerts available to your employees on a 'needs-to-know basis' strictly for your internal purposes only to assist in the protection of your information and communications technology (ICT) systems. In some instances you may be provided with Amber alerts which are marked to allow you to also disclose it to your contractors or agents on a 'needs-to-know basis' strictly for your internal purposes only to assist in the protection of your ICT systems.
Green	**Restricted to closed groups and subject to confidentiality** You may share Green alerts with external organisations, information exchanges or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the alert. You may not publish or post online or otherwise release it in circumstances where confidentiality may not be maintained.
White	**Not restricted** White alerts are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.
Not classified	Any information received from the ACSC that is not classified in accordance with the Traffic light protocol must be treated as Amber classified unless otherwise agreed in writing by the ACSC.