



Avid Technology

Apache Log4j Security Assessment

CVE-2021-44228 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>) describes a vulnerability in Apache Log4j that allows attackers to execute malicious remote code for the purpose of gaining unauthorized access to secure systems. Most organizations do not allow public access to the internet from their production environments. However, if this is not the case and your systems are exposed, you are at a higher risk for attack. When this threat was identified, Avid immediately began to investigate any potential vulnerabilities in Avid software used by our customers and our hosted environments.

This document provides information on recent or current Avid product offerings, providing a summary of the impact on these products and a description of mitigation steps where applicable. You can find this document and other security resources on the Avid Knowledge Base at: https://avid.secure.force.com/pkb/articles/en_US/troubleshooting/en239659




You can subscribe to this Knowledge Base article by selecting Subscribe under the Tools menu on the right-side of the page. After you enter your name and email address you will be notified whenever Avid updates the page with new information.




This document is subject to change as more information about the Log4j threat becomes available.

Product Impact Summary

Product	Version	Impact
Avid AirSpeed 5500	ALL	None. This product is not affected.
Avid Edit On Demand	Not Applicable	None. This product has been remediated.
Avid Editorial Management	ALL	To remediate the Log4j vulnerability, download and install the Editorial Management v2020.11.2 patch that is available on the Avid Download Center . For detailed information on these releases, see the Avid Editorial Management Documentation . This patch requires a prior installation of v2020.11.0 or later. If you are running an earlier version see “ Mitigation for Avid Editorial Management ” on page 5.
Avid Everywhere	Not Applicable	None. This product has been remediated.
Avid FastServe Ingest	ALL	None. This product is not affected.
Avid FastServe Payout	ALL	None. This product is not affected.
Avid Floating License Server	ALL	None. This product is not affected.

Product	Version	Impact
Avid ISIS	ALL	None. This product is not affected.
Avid Link	ALL	None. This product is not affected.
Avid Maestro (all products under this brand)	Not Applicable	None. This product is not affected.
Avid Media Composer	ALL	None. This product is not affected.
Avid Media Composer Distributed Processing	ALL	None. This product is not affected.
Avid MediaCentral Asset Management (includes Graphics Management, Shared Library, and Interplay MAM)	ALL	None. This product is not affected.
Avid MediaCentral Capture	ALL	None. This product is not affected.
Avid MediaCentral Cloud UX	ALL	<p>The following patches which remediate the Log4j vulnerability are available on the Avid Download Center:</p> <ul style="list-style-type: none"> • v2021.11.1 • v2021.7.6 • v2021.3.5 • v2020.9.12 • v2020.4.12 <p>For detailed information on these releases, see the Avid MediaCentral Cloud UX Documentation.</p> <p>For older versions, see “Mitigation for MediaCentral Cloud UX” on page 4 to mitigate, but not remediate the issue.</p>
Avid MediaCentral Cloud UX (Search Grid server)	ALL	None. This product is not affected.
Avid MediaCentral Command	ALL	None. This product is not affected.
Avid MediaCentral Ingest	ALL	None. This product is not affected.
Avid MediaCentral Newsroom Management (iNEWS)	ALL	<p>None. This product is not affected.</p> <p>iNEWS Web Services API and File Link: You must ensure that no one in your organization has changed the underlying Apache Tomcat from its default logger (currently JULI) to log4j.</p>
Avid MediaCentral Panel for Adobe Premiere Pro	ALL	<p>Download one of the MediaCentral Cloud UX patch releases that are listed above to remediate the Log4j vulnerability.</p> <p>Avid components installed on the Windows or macOS client are not affected by the Log4j vulnerability.</p> <p> <i>Avid did not investigate the Panels’ host application. Refer to www.adobe.com for more information.</i></p>

Product	Version	Impact
Avid MediaCentral Panel for ENPS	ALL	Download one of the MediaCentral Cloud UX patch releases that are listed above to remediate the Log4j vulnerability.  <i>Avid did not investigate the Panels' host application. Refer to www.ap.org for more information.</i>
Avid MediaCentral Production Management (Interplay Production)	ALL	None. This product is not affected.
Avid MediaCentral Stream	ALL	None. This product is not affected.
Avid MediaCentral Sync	ALL	None. This product is not affected.
Avid MediaCentral UX	ALL	None. This product is not affected.
Avid MediaCentral UX Maestro Plugin	ALL	None. This product is not affected.
Avid NEXIS	ALL	None. This product is not affected.
Avid Pro Tools	ALL	None. This product is not affected.
Avid Pro Tools Control	ALL	None. This product is not affected.
Avid Sibelius	ALL	None. This product is not affected.
Avid Sibelius Cloud Publishing (Avid Sibelius Scorch)	ALL	None. This product is not affected.
Avid VENUE	ALL	None. This product is not affected.

If you are using an Avid product that is not listed above, contact Avid Customer Care for assistance or guidance. Information might not be available for all products — including those products or product versions that have reached their End of Life, End of Sale, or End of Support dates. For more information on these dates, see https://avid.secure.force.com/pkb/articles/en_US/FAQ/End-of-support-dates.

General Mitigation and Best Practices

In general, Avid highly recommends that organizations shield their production servers from being accessible through the public internet. Systems (especially servers) should operate in a secure internal network environment by utilizing firewalls, port blocking, VPN and other secure networking means. This includes blocking outbound connections from the production servers to the Internet.

All Inbound and Outbound traffic to the Internet should be blocked. Only the Layer 4 (IP, Protocol and Port) pinholes required for normal operation to VPNs and other access networks should be open. For more information on Inbound / Outbound port usage, refer to the *Avid Port Usage Guide* at the following Avid Knowledge Base page: https://avid.secure.force.com/pkb/articles/en_US/readme/Avid-Networking-Port-Usage-Guide

If you are running an older software release of a current product, Avid highly recommends that you upgrade to take advantage of the most recent fixes and security updates that might be available in the product, or in the associated supported operating system.

Additional Resources

For more information from specific vendors, see the following links:

- CrowdStrike
<https://www.crowdstrike.com/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/>
- Microsoft
<https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/>
- VMware
<https://www.vmware.com/security/advisories/VMSA-2021-0028.html>

Mitigation for MediaCentral Cloud UX

To remediate the Log4j vulnerability in MediaCentral Cloud UX, you must upgrade to one of the patched versions under the “[Product Impact Summary](#)” on page 1. The following process serves to mitigate the threat in some cases, but it cannot completely protect your system from the Log4j issue.

Avid actively investigated MediaCentral Cloud UX back through version 2020.4.11. While Avid did not perform specific testing on releases prior to v2020.4.11, we do not expect prior versions to be negatively impacted by the following process. As general guidance for organizations running earlier versions of software, Avid recommends that you upgrade to a more current release to take advantage of the latest security fixes in both the product and the operating system.

As the following process restarts a number of pods, system administrators are encouraged to complete the following steps during a scheduled maintenance window.

To mitigate the Log4j impact for MediaCentral Cloud UX:

1. Connect to your single server or primary master node and enter the following commands:

```
kubectl set env deployment --all LOG4J_FORMAT_MSG_NO_LOOKUPS="true"
kubectl set env sts --all LOG4J_FORMAT_MSG_NO_LOOKUPS="true"
kubectl set env ds --all LOG4J_FORMAT_MSG_NO_LOOKUPS="true"
```

The system responds after each of these commands with a list of updated components. For example:

```
deployment.apps/avid-acs-attributes-core env updated
statefulset.apps/avid-resource-configsvr0 env updated
daemonset.apps/nginx-service-proxy env updated
```

2. If you deployed System Monitoring as directed by Avid, enter the following additional commands:

```
kubectl set env -n mon deployment --all LOG4J_FORMAT_MSG_NO_LOOKUPS="true"
kubectl set env -n mon sts --all LOG4J_FORMAT_MSG_NO_LOOKUPS="true"
kubectl set env -n mon ds --all LOG4J_FORMAT_MSG_NO_LOOKUPS="true"
```

As before, each command displays a list of updated components.

3. Verify that your changes have been implemented by completing the following.

a. To verify an example deployment:

```
kubectl get deployments -o yaml avid-iam-core | grep
LOG4J_FORMAT_MSG_NO_LOOKUPS
```

b. To verify an example stateful set:

```
kubectl get sts -o yaml avid-elasticsearch-search | grep
LOG4J_FORMAT_MSG_NO_LOOKUPS
```

c. To verify an example daemon-set:

```
kubectl get ds -o yaml avid-acs-gateway-default-core | grep
LOG4J_FORMAT_MSG_NO_LOOKUPS
```

d. (if applicable) To verify the monitoring updates:

```
kubectl get deployments -o yaml -n mon | grep
LOG4J_FORMAT_MSG_NO_LOOKUPS
```

Each command should reply with a message similar to the following:

```
kubectl get deployments -o yaml avid-iam-core | grep
LOG4J_FORMAT_MSG_NO_LOOKUPS
      k:{"name":"LOG4J_FORMAT_MSG_NO_LOOKUPS"}:
        - name: LOG4J_FORMAT_MSG_NO_LOOKUPS
```

The LOG4J_FORMAT_MSG_NO_LOOKUPS value confirms that the component has been upgraded. If you run any of these commands and you do not see any output, that system or that particular component was not upgraded.



If you are running MediaCentral Cloud UX v2021.11, the command reports two “NO_LOOKUPS” values. In prior releases, this command produces only one instance of the value. The monitoring verification step might also display multiple values.

Mitigation for Avid Editorial Management

To remediate the Log4j vulnerability in Avid Editorial Management, you must install the v2020.11.2 patch on your v2020.11.x server. The following process serves to mitigate the threat in some cases, but it cannot completely protect your system from the Log4j issue.

Avid actively investigated Avid Editorial Management version 2020.11. While you can complete the following process on prior releases, Avid did not perform specific testing on any version prior to v2020.11 and therefore the specific impact to prior releases is unknown. If you are running an earlier version of software, Avid recommends that organizations upgrade to a more current release to take advantage of the latest security fixes.

As the following process restarts a number of pods, system administrators are encouraged to complete the following steps during a scheduled maintenance window.

To mitigate the Log4j impact for Avid Editorial Management:

1. Using the *root* user account, sign in to the Linux virtual machine that is running on your Avid Editorial Management server using a Secure Shell (SSH) client application such as PuTTY.
2. Complete the steps as outlined in [“Mitigation for MediaCentral Cloud UX” on page 4.](#)

3. Enter the following command to reconfigure Elasticsearch:

```
echo -Dlog4j2.formatMsgNoLookups=true >> /etc/elasticsearch/jvm.options
```

4. After reconfiguring Elasticsearch, you must restart it to enable the change:

```
systemctl restart elasticsearch
```

5. Verify that Elasticsearch has been reconfigured:

- a. Enter the following command to obtain the status of the module:

```
systemctl status elasticsearch
```

Note the process's `Main` PID number for use in the following command.

- b. Enter the following command and verify the output:

```
ps aux | grep <PID_number>
```

- c. Review the output and ensure that the `elastic+` line includes the following value:

```
Dlog4j2.formatMsgNoLookups=true
```

For example (some details omitted for clarity):

```
[root@wavd-mcem ~]# ps aux | grep 588366
elastic+ 588366  8.0 /bin/java  ... -Dlog4j2.formatMsgNoLookups=true
root      744386  0.0  0.0 112788  712 pts/0    S+  --color=auto 588366
```