# Entrust Security Bulletin E21-008c

December 15, 2021

# E21-008c: Entrust Products Affected by Log4J Vulnerabilities (CVE-2021-44228, CVE-2021-45046)

## Who should read this bulletin

Entrust has triaged products for impact from CVE-2021-44228 and CVE-2021-45046. Products that have been investigated and have reached a conclusion of "Impacted" or "Not Affected" at time of publication are listed in this bulletin, along with mitigation steps. For any products not listed in this bulletin, contact Entrust Support for the most up to date information.

The following products have been found to be **Impacted** by CVE-2021-44228 and CVE-2021-45046. See below for details on each.

- Adaptive Issuance Issuance Device Management (IDM) 6.7.0, 6.7.1, 6.7.3 and 6.7.4
  *(formerly "Remote Monitoring & Management")*
- Adaptive Issuance Key Manager Software 6.6, 6.7, and 6.7.1
- Digital Signing Servers
  *(formerly "TrustedX Platform")*
- Entrust Authority Administration Services 9.3+ and 10.0+
- Entrust Authority Document Signer Service 9.0 - 9.0.30
- Entrust Authority Roaming Server 9.0
- Entrust CA Gateway (CAGW) <= 2.5
- Entrust CA Gateway ACM-PCA Plugin <= 2.5
- Entrust Certificate Enrollment Gateway (CEG) <=1.3
- Entrust Certificate Hub <= 2.2.1
- Entrust Discovery Agent <= 2.6.2
  *(the ECS cloud infrastructure is covered in bulletin E21-009)*
- Entrust IS Client 9.0
- Entrust IS Concentrator 9.0
- Entrust Key Recovery Service (KRS) Client <= 2.5
- Entrust Microsoft CA Proxy (MSCA Proxy) <= 2.5
- GetAccess Server 9.0, 9.1 and 9.2
- GetAccess Runtime 9.1
- Identity as a Service Enterprise Service Gateway (IDaaS ESG) <= 5.22
  *(the IDaaS cloud infrastructure is covered in bulletin E21-009)*
- nShield Monitor

Notes:

1. Products that have been investigated and found to be **Not Affected** are listed at the bottom of this bulletin in Appendix A.
2. All other Entrust Security Bulletins referenced below can be found here: https://trustedcare.entrust.com/articles/en_US/Security_Bulletin/Latest-Articles-regarding-Log4J-Vulnerability-for-Entrust-Products
3. Patches will be released on Trusted Care. Existing users can access Trusted Care here: https://trustedcare.entrust.com/login
    a. To setup a new Trusted Care account please email: trustedcare@entrust.com

4. Customers using older versions of these products are advised to upgrade to the latest version and apply the remediation steps described herein.

# Summary

On December 10, 2021, details emerged about a critical remote code execution vulnerability in Apache Log4j, assigned as CVE-2021-44228, in which users who can cause specifically crafted strings to be processed by an application's Log4j logging layer may be able to execute code and thereby take control of the server hosting the affected application.  On December 14, 2021, a second vulnerability in Apache Log4j, CVE-2021-45046, was identified.  This second vulnerability identifies that, despite the changes made in Log4j 2.15.0 (and the similar effect of applying an environment variable-based or system property-based mitigation), there could remain cases where arbitrary code execution could be achieved.

The official security advisory from Apache describing these issues can be found here:

- https://logging.apache.org/log4j/2.x/security.html

Entrust has investigated the impact of CVE-2021-44228 and CVE-2021-45046 on all products listed in this bulletin. Entrust is continuing to monitor and assess ongoing product impacts and will take additional action as necessary.

In the interest of releasing this bulletin in a timely manner, investigations into the details of product impacts, as well as patch availability timelines, are still ongoing. As such, information below should be considered preliminary. Entrust will release more communications, as needed, as these investigations proceed.

## Change History

| Bulletin version | Date Published | Major changes |
|---|---|---|
| E21-008 | 11 Dec 2021 | Initial release |
| E21-008a | 13 Dec 2021 | • **Added "Entrust Authority Document Signer Service" as an affected product.**<br>• Updated mitigation steps and patch availability information for several affected products:<br>  • Adaptive Issuance Key Manager Software<br>  • Entrust Authority Administration Services<br>  • Entrust CA Gateway<br>  • Entrust Certificate Enrollment Gateway (CEG)<br>  • Entrust Discovery Agent<br>  • Entrust Microsoft CA Proxy (MSCA Proxy)<br>  • GetAccess<br>  • Identity as a Service Enterprise Service Gateway (IDaaS ESG)<br>• Added Appendix A with a list of products not affected. |

| Bulletin version | Date Published | Major changes |
|---|---|---|
| E21-008b | 14 Dec 2021 | • **eConnector added to affected product list.**<br>• **Entrust Authority Roaming Server moved to affected product list.**<br>• **Entrust CA Gateway ACM-PCA Plugin added to affected product list.**<br>• Updated mitigation steps and patch availability information for several affected products:<br>  • Entrust Authority Administration Services<br>  • Entrust Certificate Hub<br>• Added products missing from Not Affected list in Appendix A:<br>  • Adaptive Issuance WebID<br>  • Administration Services on-premises components - AES Module, WNES client<br>  • Capture Manager<br>  • CRL Copier<br>  • Datacard MX Card Issuance Systems<br>  • Datacard PB Passport Issuance Systems<br>  • Data Preparation and Production (DPP)<br>  • Derived Credential Registration Service (DCRS)<br>  • Entrust Artista Printer<br>  • Entrust CD/SD Printer<br>  • Entrust Sigma Printer<br>  • Entrust TruePass<br>  • IDE Integrations - ADFS Adapter<br>  • nShield products *(formerly "nCipher")*<br>  • Syntara Manufacturing Efficiency (Syntara ME)<br>  • TransactionGuard |
| E21-008c | 15 Dec 2021 | • **IDM versions 6.7.0, 6.7.1 added to affected product list.**<br>• **nShield Monitor moved to affected product list.**<br>• All product patches are upgrading to Log4j 2.16.0 or later (previous version said "2.15 or later").<br>• Updated the Summary section to include a description of CVE-2021-45046 which was published 2021-12-14.<br>• Updated **patch availability** information for the following products:<br>  • ACM-PCA Plugin<br>  • Adaptive Issuance Key Manager Software<br>  • Entrust Authority Document Signer Service<br>  • Entrust CA Gateway<br>  • Entrust Certificate Enrollment Gateway (CEG)<br>  • Entrust Certificate Hub<br>  • IS Client<br>  • IS Concentrator<br>  • MSCA Proxy<br>• Added products missing from Not Affected list in Appendix A:<br>  • IS Client <= 8.2<br>  • IS Concentrator <= 8.1<br>  • Adaptive Issuance HSMs<br>  • IDM 6.6 |

# Table of Contents

# Impact of Vulnerability and Mitigation Steps

Products that have been investigated and have reached a conclusion of "Impacted" or "Not Affected" at time of publication are listed below. Please note that some products are still under investigation. For any products not listed in this bulletin contact Entrust Support for the most up to date information.

## Entrust Products - Impacted

This table includes Entrust products that have exposure to CVE-2021-44228. For products that are **Not Affected** please refer to **Appendix A.** As per the Apache Log4j security advisory, Entrust is expediting patches for all affected products that update Log4j to version 2.16.0 or later.

| **Product** | **Version(s)** | **Impact** | **Corrective Action**<br>*** See below for details** |
|---|---|---|---|
| Adaptive Issuance Issuance Device Management (IDM)<br>*formerly "Remote Monitoring & Management"* | 6.7.0, 6.7.1 6.7.3, 6.7.4 | Issuance Device Management uses an affected version of Log4j. | • Apply manual mitigation steps listed in the "Product Specific Updates and Instructions > Adaptive Issuance Issuance Device Management (IDM)" section below.<br>• Apply IDM patch, when available. |
| Adaptive Issuance Key Manager Software | 6.6<br>6.7, 6.7.1 | Key Manager Software uses an affected version of Log4j. | • Apply manual mitigation steps listed in the "Product Specific Updates and Instructions > Adaptive Issuance Key Manager Software" section below.<br>• Apply Key Manager 6.x Log4j2 Hotfix, when available. |
| Digital Signing Servers *(formerly "TrustedX Platform")* | <= 4.2.2.0<br><= 4.1.9.6 | TrustedX / Digital Signing Servers uses an affected version of Log4j. Investigation shows that the cases where Log4j is used to process user-controlled text do not use Log4j in a vulnerable way. The product is therefore unlikely to be affected. | • Apply TrustedX patches, when available. |
| eConnector | - | eConnector uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply eConnector patch, when available. |
| Entrust Authority Administration Services | 9.3<br>10.0, 10.1 | Administration Services uses an affected version of Log4j. This applies to the the java-based web services. It does not apply to the WNES client or AES Module, which are unaffected. | • Apply manual mitigation steps listed below.<br>• Apply Administration Services patch 9.3.52 or 10.1.22 when available. |

| Product | Version(s) | Impact | Corrective Action<br>* See below for details |
|---|---|---|---|
| Entrust Authority Document Signer Service | 9.0 | PCU, SDS, and OTCU components an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply Document Signer Service 9.0.31 when available. |
| Entrust Authority Roaming Server | 9.0 | RS package includes PCU command-line, which includes an affected version of Log4j. | • Avoid using PCU until it is patched.<br>• Apply Roaming Server patch 9.0.20 when available. |
| Entrust CA Gateway (CAGW) | <= 2.5 | CAGW uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply CAGW patch 2.5.1. |
| Entrust CA Gateway ACM-PCA Plugin | <= 2.5 | CAGW ACM-PCA Plugin uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply CAGW ACM-PCA Plugin patch 2.5.1. |
| Entrust Certificate Enrollment Gateway (CEG) | <= 1.3 | CEG uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply CEG patch 1.2.2 or 1.3.1. |
| Entrust Certificate Hub | <= 2.2.1 | Certificate Hub uses an affected version of Log4j. | • Apply Certificate Hub patch 2.2.2. |
| Entrust Discovery Agent | <= 2.6.2 | Discovery Agent uses an affected version of Log4j.<br>The exposure is appears to be limited. | • Pause scanning or apply network controls.<br>• Apply the mitigation below and plan a migration to Discovery Scanner. |
| Entrust IS Client | 9.0 | IS Client uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply IS Client patch 9.0.3 when available. |

| **Product** | **Version(s)** | **Impact** | **Corrective Action**<br>*** See below for details** |
|---|---|---|---|
| Entrust IS Concentrator | 9.0 | IS Concentrator uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply IS Concentrator patch 9.0.3 when available. |
| Entrust Key Recovery Service (KRS) Client | <= 2.5 | KRS uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply KRS patch, when available. |
| Entrust Microsoft CA Proxy (MSCA Proxy)<br>*a component of CAGW* | <= 2.5 | MSCA Proxy uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply MSCA Proxy patch 2.5.1. |
| GetAccess Server | 9.0, 9.1, 9.2 | GetAccess Server uses an affected version of Log4j. | • Apply manual mitigation steps listed below.<br>• Apply GetAccess Server patch, when available. |
| GetAccess Runtime | 9.1 | GetAccess Runtime includes an affected version of Log4j. It is not used but should be removed. | • Apply manual mitigation steps listed below.<br>• Apply GetAccess Runtime patch, when available. |
| Identity as a Service Enterprise Service Gateway (IDaaS ESG) | <= 5.22 | Potentially affected only in MS CA use cases. | • Apply manual mitigation steps listed below.<br>• Apply ESG patch, when available. |
| nShield Monitor | - | nShield Monitor uses an affected version of Log4j. | • Apply nShield Monitor patch, when available. |

# General Mitigation Steps

## Applying mitigations

As per the Apache Log4j security advisory linked to above, Entrust is expediting patches for all affected products that update Log4j to version 2.16.0 or later.

In the interim, customers can apply manual mitigation. Quoting from the Apache Log4j security page as of 2021-12-15:

> ***Log4j 2.x mitigation**: Implement one of the mitigation techniques below.*
>
> - [...]
> - Otherwise, remove the JndiLookup class from the classpath: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
>
> *[...]*
>
> *Other insufficient mitigation measures are: setting system property log4j2.formatMsgNoLookups or environment variable LOG4J_FORMAT_MSG_NO_LOOKUPS to true for releases >= 2.10*

After applying one of those mitigating steps, the service needs to be restarted.

Note that as stated in the Log4j advisory the environment variable and system property-based mitigations do not provide full protection; they are however simpler to apply and do significantly reduce risk by mitigating the issue in the most common scenarios.

In general, on Windows hosts the JndiLookup class can be removed using Windows Explorer as follows:

1. Stop the service.
2. Locate all copies of the log4j2 core jar file on the system (log4j-core-*.jar).
3. For each file:
   a. Make a backup copy of the file, storing it outside the application directories.
   b. Rename the original file, modifying the extension from .jar to .zip.
   c. Navigate inside the zip file to the `org/apache/logging/log4j/core/lookup/` directory.
   d. Delete the `JndiLookup.class` file from this directory.
   e. Rename the original file, setting the extension back to .jar.
4. Restart the service.

On Linux:

1. Stop the service.
2. Locate all copies of the log4j2 core jar file on the system (log4j-core-*.jar).
3. For each file:
   a. Make a backup copy of the log4j-core-*.jar file, storing it outside the application directories.
   b. Run the command:

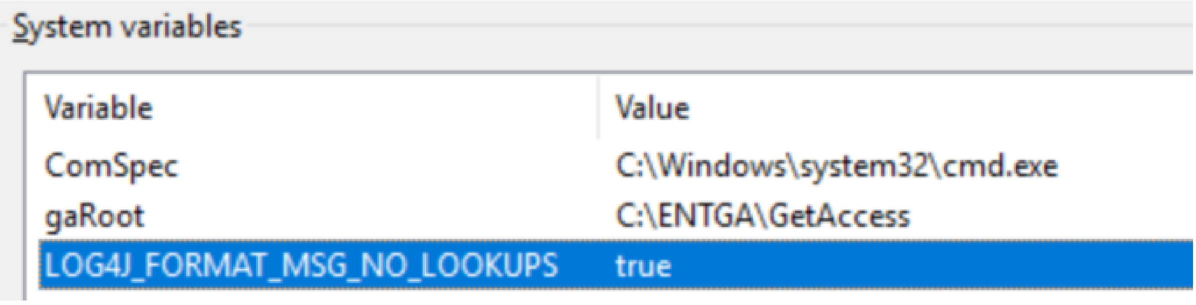
      ```
      zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/
      JndiLookup.class
      ```

      on the original jar file.
   c. Restart the service.

## Partial mitigations

Below is mitigation advice consistent with the Apache Log4j advisory prior to 2021-12-14. These mitigations are simpler to apply and do significantly reduce risk by mitigating the issue in the most common scenarios, but for full protection all products should patch to 2.16.0 or later.

In general, for applications on Windows hosts, the environment variable `LOG4J_FORMAT_MSG_NO_LOOKUPS`=true can be set system-wide in the Windows Control Panel as shown below:



System variables

| Variable | Value |
|---|---|
| ComSpec | C:\Windows\system32\cmd.exe |
| gaRoot | C:\ENTGA\GetAccess |
| LOG4J_FORMAT_MSG_NO_LOOKUPS | true |

For applications on Linux hosts, the exact steps to apply either the JVM system property (`-Dlog4j2.formatMsgNoLookups=true`) or the shell environment variable (`LOG4J_FORMAT_MSG_NO_LOOKUPS=true`) will depend on how the application is launched. In most cases, a customer would need to locate the shell script or system unit that launches the process and make the change there.

Entrust has prepared specific steps for applying these mitigations to certain products, see section "Product Specific Updates and Instructions" below.

For other products, exact mitigation steps are being investigated and will be included in an additional communication.

## Checking that mitigations are in place:

- To verify the JVM system property-based mitigation
  - **On Windows**, Microsoft's Process Explorer tool can be used to check the command line arguments used to start Java processes.
  - **On Linux**, execute the command below, replacing the string <pid> with the process id of the process of interest:

    ```
    xargs -L1 -0 -a /proc/<pid>/cmdline | grep -- -Dlog4j2.formatMsgNoLookups
    ```

    and confirm that the output shows a value of true.
- To verify the environment variable-based mitigation:
  - **On Windows**, Microsoft's Process Explorer tool can be used to check the environment variables used by a specific process.  A less complete check is possible without installing additional software:
    i. Start a new instance of the Windows command prompt.
    ii. Execute:

    ```
    echo %LOG4J_FORMAT_MSG_NO_LOOKUPS%
    ```

    The value "true" should be displayed.
    iii. Ensure that you have restarted all the affected processes.
  - **On Linux**, execute the command below, replacing the string <pid> with the process id of the process of interest:

    ```
    xargs -L1 -0 -a /proc/<pid>/environ | grep LOG4J_FORMAT_MSG_NO_LOOKUPS
    ```

    and confirm that the output shows a value of true.

# Product Specific Updates and Instructions

See below for product specific mitigation steps and additional details.

## Adaptive Issuance Issuance Device Management (IDM) 6.7.0, 6.7.1, 6.7.3, and 6.7.4

Issuance Device Management uses an affected version of Log4j prior to 2.10 and therefore the environment variable or JVM argument mitigations do not apply. The following mitigation has been tested and should be applied:

> remove the JndiLookup class from the log4j-core-*.jar file using any zip editing tool.

The following is an example of a command that can be used to remove the class:

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

Information about patches for IDM that update Log4j to version 2.16.0 or later will be included in an additional communication.

## Adaptive Issuance Key Manager Software 6.6, 6.7, and 6.7.1

Key Manager Software uses an affected version of Log4j prior to 2.10 and therefore the environment variable or JVM argument mitigations do not apply.

Key Manager 6.x Log4j2 Hotfix will update Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

The following mitigation has been tested and should be applied:

> remove the JndiLookup class from the log4j-core-*.jar file using any zip editing tool.

The following is an example of a command that can be used to remove the class:

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

## Digital Signing Servers <= 4.1.9.6, and <= 4.2.2.0

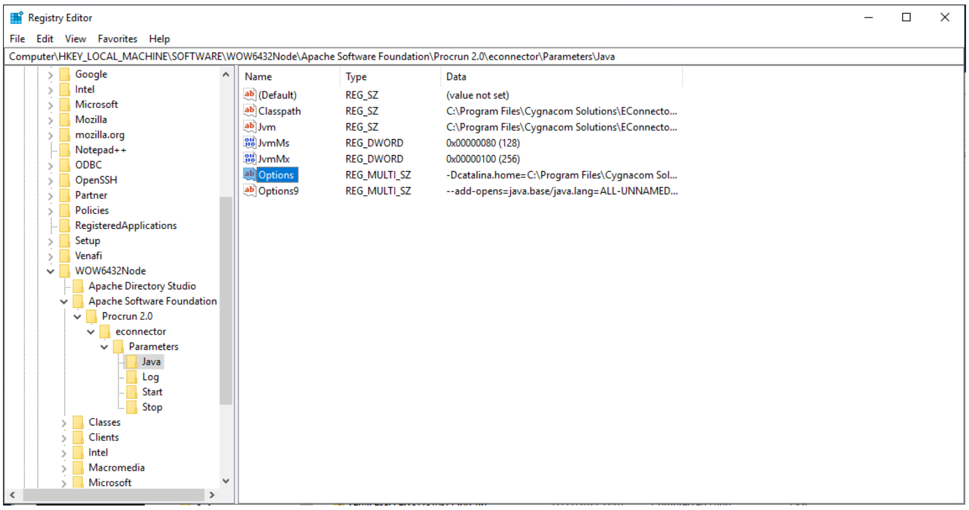
Digital Signing Servers (formerly called TrustedX Platform) use an affected version of Log4j, however early investigation shows that it is not exploitable. Investigation is ongoing.

Corrective action will be included in an additional communication.

## eConnector

eConnector uses and affected version of Log4j. Temporary mitigation by altering registry and starting the configuration tool differently as per the General Mitigation steps above.

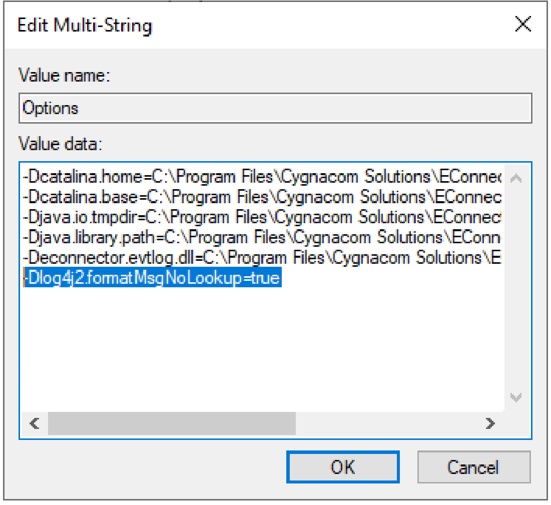
1. Using regedit, modify the Value data for **Options** located in **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\econnector\Parameters\Java**



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\econnector\Parameters\Java

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| Classpath | REG_SZ | C:\Program Files\Cygnacom Solutions\EConnecto... |
| Jvm | REG_SZ | C:\Program Files\Cygnacom Solutions\EConnecto... |
| JvmMs | REG_DWORD | 0x00000080 (128) |
| JvmMx | REG_DWORD | 0x00000100 (256) |
| Options | REG_MULTI_SZ | -Dcatalina.home=C:\Program Files\Cygnacom Sol... |
| Options9 | REG_MULTI_SZ | --add-opens=java.base/java.lang=ALL-UNNAMED... |

2. Append the Value data to include **-Dlog4j2.formatMsgNoLookup=true**



Value name:

Options

Value data:

```
-Dcatalina.home=C:\Program Files\Cygnacom Solutions\EConnec
-Dcatalina.base=C:\Program Files\Cygnacom Solutions\EConnec
-Djava.io.tmpdir=C:\Program Files\Cygnacom Solutions\EConnec
-Djava.library.path=C:\Program Files\Cygnacom Solutions\EConn
-Deconnector.evtlog.dll=C:\Program Files\Cygnacom Solutions\E
-Dlog4j2.formatMsgNoLookup=true
```

3. Click OK to save the modified Value data.
4. Restart the eConnector service.

Information about patches for eConnector that update Log4j to version 2.16.0 or later will be included in an additional communication.

## Entrust Authority Administration Services 9.3, 10.0, and 10.1

Entrust Authority Administration Services versions 9.3, 10.0, and 10.1 use an affected version of Log4j.

Administration Services version 9.3.52 and 10.1.22 will update Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

This applies to the the java-based web services. It does not apply to the WNES client or AES Module, which are unaffected.

The General Mitigation Steps listed above should be applied.

**Windows**

1. From the tomcat "bin" folder, run the following command for Administration Services 10.0 and 10.1:

```
C:\Program Files\Entrust\AdminServices\tomcat\apache-
tomcat\bin>tomcat9w.exe //ES//EntrustAdminServices
```

2. For Admin Services 9.3 patches greater than or equal to 9.3.50:

```
C:\Program Files\Entrust\AdminServices\tomcat\apache-
tomcat\bin>tomcat8w.exe //ES//EntrustAdminServices
```

3. When "Entrust Admin Services Properties" dialog box is displayed, select "Java" tab
4. Add the following line to the Java Options box:

```
-Dlog4j2.formatMsgNoLookups=true
```

5. Restart tomcat
6. Repeat the same steps for the Configuration Service:
   a. For Administration Services 10.0 and 10.1 Configuration Service:

   ```
   C:\Program Files\Entrust\AdminServices\tomcat\apache-
   tomcat\bin>tomcat9w.exe //ES//EntrustCfgws
   ```

   b. For Admin Services 9.3 patches greater than or equal to 9.3.50:

   ```
   C:\Program Files\Entrust\AdminServices\tomcat\apache-
   tomcat\bin>tomcat8w.exe //ES//EntrustCfgws
   ```

   c. When "Entrust AS Configuration Service Properties" dialog box is displayed, select "Java" tab
   d. Add the following line to the Java Options box:

   ```
   -Dlog4j2.formatMsgNoLookups=true
   ```

   e. Restart Administration Services Configuration Service

**Linux**

1. Add "log4j2.formatMsgNoLookups" JVM option to catalina.sh found in <AS_ROOT>/tomcat/apache-tomcat/bin folder. It can be anywhere in the file, for example:

```
JAVA_OPTS="$JAVA_OPTS -Djava.security.egd=...
JAVA_OPTS="$JAVA_OPTS -Dlog4j2.formatMsgNoLookups=true"
```

2. Make the same change to the configuration file <AS_ROOT>/services/cfgws/cfgws/entrust-cfgws.conf.

3. Restart the configuration service.
4. Restart the Administration Services Tomcat.

## Entrust Authority Document Signer Service 9.0

PCU, SDS, and OTCU components uses an affected version of Log4j.

VS component is unaffected is it does not use Log4j.

Document Signer Service 9.0.31 will update Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

If the patch cannot be applied immediately, then the General Mitigation Steps listed above should be applied.

## Entrust Authority Roaming Server 9.0

Entrust Authority Roaming Server 9.0 includes a java-based command-line utility Profile Creation Utility (PCU) which uses an affected version of Log4j. "pcu.bat" on Windows and "pcu" on linux.

Entrust Authority Roaming Server 9.0.20 will update Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

Due to the local nature of the PCU utility, it is highly unlikely for malicious payloads to enter the utility. Cautious users should General Mitigation Steps listed above.

## Entrust CA Gateway <= 2.5

Entrust CA Gateway up to and including 2.5 uses an affected version of Log4j.

CA Gateway 2.5.1, published on 2021-12-15, updates Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

The General Mitigation Steps listed above should be applied until the application can be patched.

## Entrust CA Gateway ACM-PCA Plugin <= 2.5

Entrust CA Gateway ACM-PCA Plugin up to and including 2.5 uses an affected version of Log4j.

CA Gateway ACM-PCA Plugin 2.5.1, published on 2021-12-15, updates Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

The General Mitigation Steps listed above should be applied until the application can be patched.

## Entrust Certificate Enrollment Gateway (CEG) <= 1.3

Entrust Certificate Enrollment Gateway up to and including 1.3 uses an affected version of Log4j.

Mitigation steps slightly differ depending on the version of Certificate Enrollment Gateway (CEG). In all cases, the following steps must be performed from the Entrust Deployment Manager (EDM) node where CEG was originally configured:

1. Once connected to the EDM node via SSH, connect to the csf-entitlements pod. The following two commands can be copy/pasted directly into the SSH session to connect to the csf-entitlements pod:

```
POD_NAME=$(kubectl get pod -n csf -l app=csf-entitlements -o
jsonpath="{.items[0].metadata.name}" --ignore-not-found)
kubectl exec -it -n csf "${POD_NAME}" --container csf-entitlements -- /
bin/bash
```

2. Modify the `ceg-deployment.yaml.template` file. This modification is the mitigation, but it won't get applied to any running ceg-application pods until CEG is restarted. This modification allows the mitigation to persist.
    a. The path to this file differs depending on the version of EDM/CEG.
        i. For versions of CEG 1.2.x or lower, the file to modify is on the `csf-entitlements` pod is: `/opt/entrust/csf/configurators/ceg/ceg-deployment.yaml.template`
        ii. For versions of CEG 1.3.x or higher, the file to modify is on the `csf-entitlements` pod is: `/opt/entrust/deployer/ceg/ceg-deployment.yaml.template`
    b. Using `vi` , add the following lines immediately below the "`env:`" line (whitespace is important - if unsure, there should be 12 spaces before the first non-whitespace character on the first line and 14 on the second line):

```
            - name: CEG_STARTUP_VARS
              value: '-Dlog4j2.formatMsgNoLookups=true'
```

3. Redeploy Certificate Enrollment Gateway. The command to redeploy differs depending on the version.

1. For versions of CEG 1.2.x or lower, run the `./clusterctl package reload` command to apply the mitigation immediately.
2. For versions of CEG 1.3.x or higher, run the `./clusterctl solution deploy` command to apply the mitigation immediately.
    a. WARNING: Do not ever provide the ceg.sln file using the '-f'/'--solution' option as that will revert/undo the mitigation changes performed above.

To simplify the above steps, a script (ceg-log4j-vuln-mitigation.sh available on TrustedCare) has been provided which can automate steps 1 and 2. The script has been validated against both CEG 1.3 and CEG 1.2. To use the script, copy the file over to the EDM node where CEG was originally installed, and then perform the following steps from that EDM node:

1. Change the permissions of the file to make it executable and run the script. For example: `chmod +x ./ceg-log4j-vuln-mitigation.sh && ./ceg-log4j-vuln-mitigation.sh`
2. After running the script, CEG must still be manually redeployed as per step #3 above.

Certificate Enrollment Gateway version 1.2.2 and 1.3.1, published on 2021-12-15, update Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

## Entrust Certificate Hub <= 2.2.1

Entrust Certificate Hub up to and including 2.2.1 uses an affected version of Log4j.

Certificate Hub patch 2.2.2, published on 2021-12-15, updates Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

## Entrust Discovery Agent <= 2.6.2

Entrust Discovery Agent (which is out of support and superseded by Entrust Discovery Scanner) uses an affected version of Log4j. As Discovery Agent is out of support, patches will not be produced. Customers may manually apply the mitigation steps below, or upgrade to the newer Discovery Scanner product.

The exposure appears to be limited, but Entrust recommends performing the following steps to mitigate the issue.

1. Navigate to the Discovery Agent installation folder (default location "C:\Program Files (x86)\Entrust\Discovery-Agent\")
2. Edit the startup file "bin\service.bat" to add the following bolded line to the beginning of the file:

```
@echo off
set LOG4J_FORMAT_MSG_NO_LOOKUPS=true
```

3. Restart the Discovery Agent.

Discovery Scanner is unaffected.

The Entrust Certificate Services cloud platform not affected, and is covered in Entrust Security Bulletin E21-009.

## Entrust IS Client 9.0

Entrust IS Client (a standalone component of the ePassport solution) version 9.0 uses an affected version of Log4j.

IS Client 9.0.3 will update Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

The General Mitigation Steps listed above should be applied.

## Entrust IS Concentrator 9.0

Entrust IS Concentrator (a standalone component of the ePassport solution) version 9.0 uses an affected version of Log4j.

IS Concentrator 9.0.3 will update Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

The General Mitigation Steps listed above should be applied.

Information about patches for IS Concentrator that update Log4j to version 2.16.0 or later will be included in an additional communication.

## Entrust Key Recovery Service (KRS) Client <= 2.4, and 2.5

Entrust Key Recovery Service Client version up to 2.4 and 2.5 uses an affected version of Log4j.

Note that the Entrust-hosted server instance has had mitigations applied as per the mPKI statement in Entrust Security Bulletin E21-008.

The General Mitigation Steps listed above should be applied.

Information about patches for KRS that update Log4j to version 2.16.0 or later will be included in an additional communication.

## Entrust Microsoft CA Proxy (MSCA Proxy) <= 2.5

Entrust Microsoft CA Proxy (a standalone component of CAGW) up to and including 2.5 uses an affected version of Log4j.

CA Gateway MSCA Proxy 2.5.1, published on 2021-12-15, updates Log4j to version 2.16.0. All patches are posted on TrustedCare when they become available.

The General Mitigation Steps listed above should be applied.

## GetAccess Server 9.0, 9.1, and 9.2

GetAccess Server 9.0 patch 207505, 9.1 and 9.2 use an affected version of Log4j and are known to be directly exposed to CVE-2021-44228. Customers are urged to apply immediate mitigations as documented in Entrust Security Bulletin E21-010.

## GetAccess Runtime 9.1

GetAccess Runtime 9.1 includes an affected version of Log4j.  While the product does not call the library, Entrust recommends that GetAccess customers delete the jar file from runtime systems.  Please see Entrust Security Bulletin E21-010 for mitigation advice.

## Identity as a Service Enterprise Service Gateway (IDaaS ESG) <= 5.22

The IDaaS Enterprise Service Gateway includes a version of Entrust CA Gateway which is used to issue Smart Credentials from an on-premises Microsoft CA. Customers who are using a Microsoft CA will also have the Entrust MS CA Proxy deployed in their environment.  Both of these products contain a version of log4j that makes them vulnerable.  Customers who have a Microsoft CA configured in their IDaaS account may be vulnerable although Entrust has been unable to generate a scenario where user provided input results in logs being generated by Entrust CA Gateway. To completely mitigate the vulnerability to Entrust CA Gateway in the Enterprise Service Gateway, the customer should perform the following procedure on their ESG:

- log in to their ESG
- run the following command:

  ```
  sudo systemctl edit cagw.service
  ```

  This will start a text editor.
- Enter the following value and save the file:

  ```
  [Service]
  Environment="LOG4J_FORMAT_MSG_NO_LOOKUPS=true"
  ```

- run the following command to restart the service

```
sudo systemctl restart cagw.service
```

To mitigate the vulnerabilities for the Microsoft CA Proxy application that accompanies ESG, see the corresponding section above.

An upcoming release of ESG will upgrade to versions of Entrust CA Gateway and MS CA Proxy that updates Log4j to 2.16.0 or later.

### nShield Monitor

nShield Monitor up uses an affected version of Log4j.

Information about patches for nShield Monitor that update Log4j to version 2.16.0 or later will be included in an additional communication.

Note that nShield Monitor cannot make any changes to either HSMs or nShield Clients.

## Mitigating Factors

- Exploitation of CVE-2021-44228 requires that an attacker cause the server running Log4j to open a network connection to a remote host running a malicious application. It is possible to protect application servers running vulnerable Log4j implementations by implementing network controls that prevent that server from opening connections to untrusted networks or hosts.
  An example of such a policy would be to use onboard firewall software, or network zone firewalls to prevent servers from opening connections to the internet. Please work with your network and technology teams as blocking outgoing connections may affect legitimate functionality of a server or application.

## Support

Entrust Support can be contacted using our standard methods:

- Email: support@entrust.com
- Support Portal: https://trustedcare.entrust.com/login
- Phone: support numbers

Given the very nature of security vulnerabilities, security bulletins are intended to be kept to a small group of individuals. Security bulletins are to be distributed within your company only, and only on a need to know basis.

The information in this bulletin is proprietary and confidential to Entrust Corporation. and its subsidiaries, and any disclosure of this information is governed by the confidentiality terms in the agreement pursuant to which you obtained a license for the referred to Entrust products.

The information in this bulletin is provided "as is" by Entrust without any representations, conditions and/or warranties of any kind, whether express, implied, statutory, by usage of trade, or otherwise. Entrust specifically disclaims any and all representations, conditions, and/or warranties of merchantability, satisfactory quality, and/or fitness for a particular purpose. To the maximum extent permitted by applicable law, in no event will Entrust be liable for any damages, losses or costs arising from your or any third party actions or omissions in connection with this bulletin. The only representations, conditions and/or warranties that may be applicable to any Entrust products that you may have are those contained in the agreement pursuant to which you obtained a license for those Entrust products.

## Appendix A: Entrust Products - Not Affected

Entrust has determined that the following products are unaffected. For any products not listed in this bulletin, contact Entrust Support for the most up to date information.

| Product | Version(s) | Analysis | Status |
|---|---|---|---|
| Adaptive Issuance<br>- Adaptive Issuance Chip Interface Software (All released versions)<br>- Adaptive Issuance Chip Interface Software Development Kit (All released versions)<br>- Adaptive Issuance Open Perso Software (All released versions)<br>- Adaptive Issuance Open Perso Software Development Kit (All released versions)<br>- Adaptive Issuance Job Enable Software (All released versions)<br>- Adaptive Issuance Job Enable Software Development Kit (All released versions)<br>- Adaptive Issuance Data Access Software (All released versions)<br>- Adaptive Issuance Data Access Software Development Kit (All released versions)<br>- Adaptive Issuance Key Manager Software (versions 8.2.2 and 8.2.3, and versions prior to 6.6) *See section "Impacted products" for affected versions*<br>- Adaptive Issuance Firmware for SafeNet® HSMs (All released versions)<br>- Adaptive Issuance EMV Data Prep and Perso Software (All released versions)<br>- Adaptive Issuance EMV Profile Manager Software (All released versions)<br>- Adaptive Issuance EMV Runtime Software (All released versions)<br>- Adaptive Issuance MULTOS Data Prep and Perso Software (All released versions)<br>- Adaptive Issuance MULTOS Runtime Software (All released versions)<br>- Adaptive Issuance MULTOS MSM Automation Software (All released versions) | -- | Either do not use Log4j, or includes Log4j 1.x but does not use a JMS Appender<br>Note that Key Manager Software 6.6, 6.7, and 6.7.1 ***are affected***, see above. | Not Affected |

| Product | Version(s) | Analysis | Status |
|---|---|---|---|
| • Adaptive Issuance Batch Data Prep Software (All released versions)<br>• Adaptive Issuance WebID | | | |
| Adaptive Issuance HSMs (nShield HSM*i* and ProtectServer) | nShield HSM*i* 8000, nShield HSM*i* 16000, PL25, PL1500 | nShield HSM*i* does not use Log4j. ProtectServer status is based on communication from Thales. | Not Affected |
| Adaptive Issuance Instant Financial Issuance CardWizard Core | All released versions (6x and 8x streams) | Does not use Log4j | Not Affected |
| Adaptive Issuance Issuance Device Management (IDM)<br>*See section "Impacted products" for affected versions* | 6.6; 6.8 and above | Either does not use Log4j, or includes Log4j 1.x but does not use a JMS Appender<br>Note that IDM 6.7.0, 6.7.1, 6.7.3 and 6.7.4 ***are affected***, see above. | Not Affected |
| Adaptive Issuance Instant Financial Issuance Endpoint Agent<br>• Endpoint Agent Installer<br>• Extension Manager Service (Remote)<br>• Secure Issuance Proxy Service<br>• Trusted Endpoint Service<br>• Legacy TCP AddOn Service | All released versions (8x stream) | Does not use Log4j | Not Affected |
| Adaptive Issuance Instant Financial Issuance<br>• Device Dispatcher Service (DDS) Installer<br>• Batch Input Client (non-Web)<br>• Migration Tool (Import/Export) | All released versions (8x stream) | Does not use Log4j | Not Affected |
| AirWatch Derived Credential Bridge (ADC Bridge)<br>*(formerly "Airwatch Data Connect Bridge")* | All released versions | Does not use Log4j | Not Affected |
| Capture Manager | All released versions | Does not use Log4j | Not Affected |

| Product | Version(s) | Analysis | Status |
|---|---|---|---|
| CRL Copier | All released versions | Includes Log4j 1.x but does not use a JMS Appender | Not Affected |
| Datacard MX Card Issuance Systems | All released versions | Does not use Log4j | Not Affected |
| Datacard PB Passport Issuance Systems | All released versions | Does not use Log4j | Not Affected |
| Data Preparation and Production (DPP) | All released versions | Does not use Log4j | Not Affected |
| Derived Credential Registration Service (DCRS)<br>*(formerly "Derived Credential Revocation Service")* | All released versions | Does not use Log4j | Not Affected |
| Entrust Artista Printer | All released versions | Does not use Log4j | Not Affected |
| Entrust Authority Administration Services<br>*See section "Impacted products" for affected versions* | <= 8.3 | Some components include Log4j 1.x but does not use a JMS Appender<br>Note that Administration Services 9.3+ and 10.0+ ***are affected***, see above. | Not Affected |
| Entrust Authority Administration Services on-premises components:<br>• AES Module<br>• WNES client | All released versions | Does not use Log4j | Not Affected |
| Entrust Authority Enrollment Server for Web | All released versions | Does not use Log4j | Not Affected |
| Entrust Authority IS Client | <= 8.2 | Includes Log4j 1.x but does not use a JMS Appender<br>Note that IS Client 9.0 ***is affected***. See above. | Not Affected |

| Product | Version(s) | Analysis | Status |
|---|---|---|---|
| Entrust Authority IS Concentrator | <= 8.1 | Includes Log4j 1.x but does not use a JMS Appender<br>Note that IS Concentrator 9.0 ***is affected***. See above. | Not Affected |
| Entrust Authority Security Manager | All released versions | Does not use Log4j | Not Affected |
| Entrust Authority Security Administration Toolkit for Java | All released versions | Does not use Log4j | Not Affected |
| Entrust Authority Security Toolkit for the Java Platform | All released versions | Does not use Log4j | Not Affected |
| Entrust CD/SD Printer | All released versions | Does not use Log4j | Not Affected |
| Entrust EMV Personalization Validation Software (All released versions) | All released versions | Does not use Log4j | Not Affected |
| Entrust Identity Enterprise *(formerly "IdentityGuard")*<br>• Self-Service Module<br>• Print Module<br>• Federation Module<br>• Enrollment Module | All released versions (<= 13.0) | Some components include Log4j 1.x but does not use a JMS Appender | Not Affected |
| Entrust Identity Integrations, used with Identity Enterprise, and Identity-as-a-service *(formerly "IdentityGuard Integrations")*<br>• ADFS Adapter<br>• Apache Filter<br>• OAM<br>• SiteMinder<br>• ISAM<br>• ForgeRock | All released versions | Either do not use Log4j, or includes Log4j 1.x but does not use a JMS Appender | Not Affected |

| Product | Version(s) | Analysis | Status |
|---|---|---|---|
| Entrust Identity Enterprise Desktop Credential Provider<br>*(formerly "Desktop Credential Provider")* | All released versions | Does not use Log4j | Not Affected |
| Entrust Identity Essentials<br>*(formerly "SMS Passcode")* | All released versions | Does not use Log4j | Not Affected |
| Entrust Identity Android app | All released versions (<= 21.10.0) | Includes Log4j 1.x but does not use a JMS Appender | Not Affected |
| Entrust Identity iOS app | All released versions | Does not use Log4j | Not Affected |
| Entrust Mobile Soft Token SDK Android | All released versions (<= 3.5) | Includes Log4j 1.x but does not use a JMS Appender | Not Affected |
| Entrust Mobile Smart Credential SDK Android | All released versions (<= 3.7) | Includes Log4j 1.x but does not use a JMS Appender | Not Affected |
| Entrust Entelligence Security Provider for Windows | All released versions | Does not use Log4j | Not Affected |
| Entrust Entelligence Secure Desktop for Mac | All released versions | Does not use Log4j | Not Affected |
| Entrust Sigma Printer | All released versions | Does not use Log4j | Not Affected |
| Entrust TruePass | All released versions | Includes Log4j 1.x but does not use a JMS Appender | Not Affected |
| HyTrust CloudControl | All released versions | Includes Log4j 1.x but does not use a JMS Appender | Not Affected |

| Product | Version(s) | Analysis | Status |
|---|---|---|---|
| HyTrust KeyControl | All released versions | Does not use Log4j | Not Affected |
| HyTrust DataControl | All released versions | Does not use Log4j | Not Affected |
| HyTrust Vitals | All released versions | Includes Log4j 1.x but does not use a JMS Appender | Not Affected |
| ID Works / ID Centre | All released versions | Does not use Log4j | Not Affected |
| Instant ID (IID)<br>*(formerly "TruCredential")* | All released versions | Does not use Log4j | Not Affected |
| nShield HSM Firmware<br>*(formerly "nCipher")* | All released versions | Does not use Log4j | Not Affected |
| nShield Connect<br>*(formerly "nCipher")* | All released versions | Does not use Log4j | Not Affected |
| nShield Host Software<br>*(formerly "nCipher")* | All released versions | Does not use Log4j | Not Affected |
| nShield sqlekm<br>*(formerly "nCipher")* | All released versions | Does not use Log4j | Not Affected |
| nShield TimeStamp Option Pack<br>*(formerly "nCipher")* | Latest | Does not use Log4j<br>*Older versions are still under investigation.* | Not Affected |
| nShield WSOP v2+<br>*(formerly "nCipher")* | All released versions | Does not use Log4j | Not Affected |
| Production Analytics Solution (PAS) | All released versions (<= 2.4) | Does not use Log4j | Not Affected |

| Product | Version(s) | Analysis | Status |
|---|---|---|---|
| SafeLayer KeyOne | All released versions | Does not use Log4j | Not Affected |
| Secura | All released versions | Does not use Log4j | Not Affected |
| Syntara Manufacturing Efficiency (Syntara ME) | All released versions | Does not use Log4j | Not Affected |
| TransactionGuard | All released versions | Includes Log4j 1.x but does not use a JMS Appender | Not Affected |
| WorldReach IDV, PassportReach, CrisisReach and AssistReach | All released versions | Does not use Log4j | Not Affected |