Axway Security Notice

eMudhra (emSign) certificate authority key compromise — impact on Axway API Gateway and API Manager

Related CVE: CVE-2026-114820 (Java/JSSE, CVSS v3.1 9.1 Critical) and CVE-2026-91403 (JSSE, CVSS v3.1 9.1 Critical) • Issued 28 October 2026 • Revision 1.0

Item	Detail
Affected products	Axway API Gateway and Axway API Manager (currently supported 7.7 versions)
Affected component	Azul Zulu JRE bundled with the product — trust store (cacerts)
Nature of the issue	Trust store contains certificate authority roots whose subordinate CA private keys are publicly recoverable
Risk	Acceptance of forged TLS server certificates, enabling impersonation or man-in-the-middle of outbound connections
Severity	Critical — the related Java vulnerability CVE-2026-114820 is scored 9.1 by Oracle
Exploitation status	Compromised keys publicly demonstrated; no exploitation of Axway customer environments reported to Axway at time of issue
Customer action required	Yes — see sections 5 and 6

1. Summary

In October 2026 it became public that the private keys of eight intermediate certificate authority (CA) certificates operated by eMudhra, trading as “emSign”, can be recovered by anyone from the published certificates alone. Anybody holding those keys can issue TLS certificates that any system still trusting the eMudhra chain will accept as valid.

Axway API Gateway and API Manager ship with an Azul Zulu Java runtime whose trust store includes the four emSign root CA certificates that those compromised intermediates chain to. Java does not check certificate revocation by default, so an unpatched runtime will accept a forged certificate issued under one of the compromised intermediates. This affects connections the gateway makes outbound over TLS, for example to backend APIs, identity providers, and other external endpoints.

This is not a defect in Axway code. It is a compromise of a third-party certificate authority that is trusted by default in the bundled Java runtime, as it is in most Java runtimes and operating systems. Remediation consists of removing that trust, and of checking whether your own configuration or your own certificates depend on the affected CA.

Axway recommends that API Gateway and API Manager customers assess their exposure now using section 4, and plan remediation per section 5.

2. What happened

On 30 April 2025, eMudhra generated eight intermediate CA certificates — six authorised to issue TLS certificates and two authorised for code signing. A flaw in the key-generation ceremony script produced a second, weak key pair alongside the properly generated one. The weak keys carried labels resembling the legitimate ones and were mistakenly used to sign the production certificates. Each resulting private key is nominally a P-384 elliptic-curve key, but the actual secret value is a small number below 256 instead of a long random value. One recovered key's value was the number 4.

A researcher reported this on 17 October 2026 and the details were published on 20 October. Chrome and Firefox blocked the certificates within hours using their live blocklist mechanisms, Apple followed on 19 October and Microsoft on 20 October. eMudhra and Sectigo, which had cross-signed all eight intermediates under its "AAA Certificate Services" root in May 2025, revoked them. In total 20 certificates are implicated: 4 roots and 16 intermediates.

The practical problem for server software is that browsers receive blocklist updates out of band and enforce Certificate Transparency, so they reject the compromised certificates regardless. Most non-browser TLS clients do neither. They load a CA bundle from disk at start-up, or have it compiled in, and trust its contents until the bundle, library, or runtime is explicitly updated and the process is restarted. There is no live push mechanism. A bundled Java trust store is exactly this kind of static trust source, and it does not appear as a versioned dependency in a software bill of materials, which is why it can survive operating system and runtime patching unnoticed.

3. Affected Axway API Management products

3.1 Bundled Java runtime trust store

The Azul Zulu JRE bundled with API Gateway and API Manager contains the following trusted root entries in its cacerts trust store:

Alias	Subject
comodoaaaca [jdk]	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB
emsigneccrootcag3 [jdk]	CN=emSign ECC Root CA - G3, O=eMudhra Technologies Limited, OU=emSign PKI, C=IN
emsignrootcag2 [jdk]	CN=emSign Root CA - G2, O=eMudhra Technologies Limited, OU=emSign PKI, C=IN
emsignrootcag1 [jdk]	CN=emSign Root CA - G1, O=eMudhra Technologies Limited, OU=emSign PKI, C=IN

These are the four roots that the compromised intermediates chain to. Their presence was confirmed by inspection of a running API Gateway container on version 7.7.20260228, and the same trust anchors are present in the Java runtime shipped with the currently supported 7.7 releases. Older releases from 2024 or earlier could find the following 2 compromised roots.

Alias	Subject
cert_92_emsign_ecc_root_ca___c392	CN=emSign ECC Root CA - C3, O=eMudhra Inc, OU=emSign PKI, C=US
cert_91_emsign_root_ca___c191	CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US

Axway recommends that you verify your own deployment using the commands in section 4 rather than assuming a particular result.

The Sectigo “AAA Certificate Services” root, which cross-signed the same eight intermediates, was not found in the bundled trust store. The cross-signed path is therefore not trusted through the bundled Java runtime. It may still be trusted by other trust stores in your environment, including the host operating system bundle and any application-specific stores, so it should be included in your wider review.

3.2 Affected versions

- API Gateway and API Manager 7.7.20260228 (February 2026)
- API Gateway and API Manager 7.7.20260530 (May 2026)
- API Gateway and API Manager 7.7.20260830 (August 2026)
- Earlier 7.7 releases that remain in support, which ship a Java runtime predating the fix

Both classic software installations and container deployments are affected, because both use the Java runtime delivered with the product.

3.3 Exposure beyond the bundled runtime

Three further areas of your deployment can carry the same trust and should be reviewed alongside the Java runtime:

- **Certificates imported into your gateway configuration.** eMudhra or emSign certificates may have been imported into the API Gateway certificate store or the API Manager certificate store, where they are held in the configuration database. These are independent of the Java trust store and are not addressed by a product update.
- **Your own server and client certificates.** If any certificate used by your API Gateway listeners, or by your outbound mutual TLS connections, was issued under one of the affected eMudhra intermediates, it has been revoked by the CA and must be replaced.
- **Other trust stores on the host.** The host operating system CA bundle, container base image bundles, and any trust store used by components alongside the gateway each need to be patched by their own vendor or distribution.

3.4 Other Axway products

Axway’s Software Security Group has asked every product team to assess the use of certificate trust stores in their products, because CA bundles are data files rather than versioned dependencies and so are not surfaced by software composition analysis. Assessments for other Axway products are published separately. Axway SecureTransport customers should refer to the knowledge base article at https://support.axway.com/kb/195100/language/en.

4. Assessing your exposure

4.1 Check the bundled Java trust store

On a classic installation, run the following against the Java runtime used by your API Gateway, substituting the keytool and cacerts paths for your installation:

```
keytool -list -v -keystore <JAVA_HOME>/lib/security/cacerts \
  -storepass changeit 2>/dev/null | grep -iE "emSign|AAA Certificate"
```

For a containerised deployment on Kubernetes, the following locates the runtime and lists the relevant entries in a running pod:

```
kubectl exec -n <namespace> <pod> -- sh -c \
  'k=$(find / -name keytool -type f 2>/dev/null | head -1); \
   c=$(find / -name cacerts -type f 2>/dev/null | head -1); \
   $k -list -v -keystore $c -storepass changeit 2>/dev/null \
   | grep -iE "emSign|AAA Certificate"'
```

Any emSign alias returned means the runtime still trusts an affected root. Note that a deployment may contain more than one Java runtime; check each one that the product uses.

4.2 Check certificates in your gateway configuration

List the certificates held in your API Manager environment and review them for eMudhra or emSign issuers:

```
apim api check-certs -s <api-env> -days 100000
```

Also review the API Gateway certificate store in Policy Studio, and any truststores referenced by your SSL interfaces and connection policies. Axway is aware that customers with large numbers of API integrations need a bulk method of identifying affected entries and is preparing guidance for this; please see this Knowledge based article for details – https://support.axway.com/kb/195160/language/en

4.3 Verify against the published certificate list

The incident tracking site at https://emudhra.we-have-a-problem.com/ publishes the full list of the 4 root and 16 intermediate certificates with their hashes. Use it to confirm matches found in your environment. The same site maintains a list of patched operating systems, distributions, root store bundles, language runtimes, and applications.

5. Remediation of the bundled Java runtime

5.1 Product updates

Azul has released Zulu builds that address the compromise. Axway is updating the Java runtime bundled with API Gateway and API Manager to an Azul Zulu build that carries the fix. The update is

targeted for the November 2026 release (7.7.20261130) and will be identified in that release's release notes. Delivery of the same update to earlier supported versions is currently in progress.

Applying the product update is the complete and supported remediation for the bundled runtime. Customers who cannot wait for it should read section 5.2.

5.2 Interim measures

Two interim approaches exist for a Java runtime that has not yet been updated:

- **Remove the affected roots from the trust store.** Delete the four emSign aliases listed in section 3.1 from the runtime's cacerts using keytool -delete, keeping a backup of the original file, and restart the gateway. This is the approach the later Java updates take. Only do this if you are certain that no legitimate connection in your environment depends on an emSign-issued certificate.
- **Apply Azul's block list file.** Azul publishes a replacement blocked.certs file, with instructions for classic installations and container images, at https://docs.azul.com/core/release/october-2026-respin/emudhra-workaround. Important: Azul now states that this workaround no longer fully addresses the problem and that customers should update to the latest release instead (see section 6).

In both cases, make the change to the image or the deployment rather than to a running container, so that the change survives a restart or a rescheduled pod, and restart every process that uses the runtime. Validate in a non-production environment first, confirming that your outbound connections to backend APIs and identity providers still complete successfully.

Note that these interim measures will be reverted by a later runtime update that does not itself contain the fix, so re-check the trust store after any change to the runtime.

5.3 Certificates in your configuration and your own certificates

- Remove any eMudhra or emSign certificate you have imported into the API Gateway or API Manager certificate stores, unless you have confirmed it is unaffected and still required.
- Replace any certificate in use in your environment that was issued under one of the affected intermediates. Those certificates have been revoked by the CA and by the browser and operating system vendors, so they will progressively fail elsewhere regardless of the gateway configuration.
- Where a backend endpoint you connect to presents an affected certificate, ask its operator to re-issue from an unaffected CA. Do not add a trust exception as a workaround.

6. Why the first Java fix was not sufficient

The first round of Java updates, published on 21 October 2026, added the eight compromised intermediate certificates to the runtime's block list, the blocked.certs file in JDK 11 and later. Shortly afterwards a related weakness was identified, tracked as CVE-2026-114820 and scored 9.1 by Oracle in the JSSE component. Oracle's security alert states that the fix removes the set of affected eMudhra root CA certificates altogether, rather than relying on blocking the known intermediates.

Azul published a second out-of-cycle update on 24 October 2026 for Zulu 25, 21, 17, 11, 8, 7 and 6, and has added a warning to its workaround page stating that the block list workaround no longer fully addresses the problem and that customers should update to the latest release. Any assessment of Java exposure written before 24 October 2026 may describe builds as fixed that are not.

Axway is taking this into account when selecting the Azul Zulu build to bundle, so that the version shipped carries the complete fix rather than the initial block list change.

7. What Axway is doing

- Axway's Software Security Group issued an internal impact listing on 22 October 2026 requiring every product team to assess how certificate trust stores are used in their products, and is tracking the responses.
- The API Management team has confirmed the presence of the affected emSign roots in the bundled Java runtime trust store and the absence of the Sectigo cross-signing root.
- An updated Azul Zulu runtime is being integrated and validated for API Gateway and API Manager.
- Axway is preparing guidance for identifying affected certificates held in API Manager configuration at scale.
- This notice will be revised as the runtime update and that guidance become available.

8. Frequently asked questions

Is my API Gateway vulnerable to a remote attack because of this?

The exposure is to interception rather than to direct compromise of the gateway. An attacker holding one of the recovered keys, and in a position to intercept or redirect traffic, could present a forged certificate that an unpatched runtime would accept. That allows impersonation of an endpoint your gateway connects to, and interception of the data exchanged with it.

Do I need to upgrade API Gateway to fix this?

The supported fix arrives with an updated bundled Java runtime in a product release. If you cannot wait for it, discuss the interim measures in section 5.2 with Axway Support before applying them.

Will removing the emSign roots break anything?

Only connections that depend on a certificate issued by emSign, which is a small CA. Browser and operating system vendors have already removed or blocked this trust, so such connections are failing elsewhere already. Verify your outbound endpoints in a test environment before changing production.

I patched my operating system. Is that enough?

No. The Java runtime delivered with the product carries its own trust store and is not updated by operating system patching. Both need to be addressed, along with any trust store held in your gateway configuration.

Why did this not appear in a vulnerability scan or an SBOM?

Certificate bundles are data files inside a package rather than versioned dependencies, so software composition analysis does not report them and they carry no version tied to the fix. This is why Axway is assessing them by inspection rather than by scan.

Has Axway seen any exploitation of customer environments?

No exploitation of Axway customer environments has been reported to Axway at the time this notice was issued.

9. References

- Incident tracking site, including the full certificate and hash lists: https://emudhra.we-have-a-problem.com/
- Oracle Security Alert for CVE-2026-114820: https://www.oracle.com/security-alerts/alert-cve-2026-114820.html
- Azul Zulu out-of-cycle update release notes, 24 October 2026: https://docs.azul.com/core/release-notes
- Azul Zulu eMudhra workaround, including the warning on its sufficiency: https://docs.azul.com/core/release/october-2026-respin/emudhra-workaround
- Endor Labs analysis of trust stores affected by the compromise: https://www.endorlabs.com/learn/emudhra-intermediate-ca-compromise-the-trust-stores-you-patched-and-the-ones-you-didnt-know-you-had
- Red Sift analysis: https://redsift.com/blog/emudhra-ca-key-compromise
- SafeDep analysis: https://safedep.io/emudhra-ca-key-compromise/
- Axway SecureTransport knowledge base article: https://support.axway.com/kb/195100/language/en

10. Contacting Axway

For assistance with this notice, or to confirm the remediation path for your environment, open a case with Axway Support through Axway Support Central. If you already have a case open on the eMudhra CA compromise, please continue to use it so that updates reach you directly.

When contacting Support, please have the following ready: your API Gateway and API Manager versions, your deployment type (classic installation, container images, or Axway-managed cloud), the output of the trust store checks in section 4, and whether you have knowingly imported eMudhra or emSign certificates into your configuration.

This notice is provided for the information of Axway customers and reflects Axway's assessment as of the issue date. Guidance on this incident has changed more than once since disclosure, and this notice will be updated as further information becomes available. Revision 1.0 — 28 October 2026.