Java JSSE: eMudhra CA Vulnerabilities

Several intermediate CA certificates issued by eMudhra were compromised and revoked on 18 October 2026. Java does not check certificate revocation by default, so Oracle released two Security Alerts for the JSSE component of Oracle Java SE and GraalVM: CVE-2026-91403 distrusts eight compromised intermediate CA certificates and their cross-signs, and CVE-2026-114820 removes the affected eMudhra and Sectigo root CA certificates from the Java trust store. Both are rated Critical (CVSS 9.1). An attacker holding such a certificate could impersonate any server or peer in TLS connections established by an affected Java runtime.

Several dormakaba products use an affected Java runtime or trust store. For dormakaba-hosted cloud services, dormakaba applies the fixes and no customer action is required. MATRIX (MATRIX ONE, MATRIX Professional), B-COMM HCM, B-COMM ERP and B-COMM 7 are operated by the customer and require the customer to apply a fix. For the resivo Android app and the Access Manager AC30, customers should take the measures described in the Mitigations section. All other listed products have a low risk and require no customer action. See section Mitigations for details.

Advisory Information

ID:	DKSA-26-16-111	
CVE Numbers and Scores:	CVE-2026-91403	9.1 (Critical)
	CVE-2026-114820	9.1 (Critical)
Published:	16 November 2026	
Advisory Version:	1	

Affected Products

- MATRIX (MATRIX ONE, MATRIX Professional, MATRIX Cloud)
- B-COMM HCM/7/ERP
- resivo (Android app)
- Wireless Gateway 90 40-K5/K7
- Wireless Gateway exivo 90 42-K7
- Periphery Connector (PeCo) 92 32-K5, 90 42-K5
- B-Client AC30-K7
- Terminals 96 00-K7/98 00-K7

Recommendation

The recommendation depends on the Estimated Risk of the respective product as listed in the Mitigations table. The table below shows the recommended timeframe for each Estimated Risk level.

Risk	Recommendation
High/Critical	Updates should be applied as soon as possible based on organizational needs and threat model.
Medium	Within six months, based on organizational needs and threat model.
Low	During the next scheduled update cycle or within a year.
None / Info	Based on organizational needs and after appropriate testing.

Mitigations

Product	Estimated Risk	Customer Action
MATRIX (MATRIX ONE, Professional)	Critical	Run the executable fix tool or install the fixed release (see Mitigation Details), as soon as possible.
MATRIX Cloud	None/Info	dormakaba has applied the required fixes. No customer action is required.
B-COMM HCM	Critical	Run the script provided by dormakaba or install version 2026.2.3 once available.
B-COMM 7	Critical	Run the script provided by dormakaba.
B-COMM ERP	Critical	Run the script provided by dormakaba.
resivo (Android app)	Medium	Keep Android devices up to date. Optionally, deactivate the eMudhra (emSign) certificates in the Android trusted credentials settings. The iOS app requires no action. The resivo cloud services are not affected.
Wireless Gateway 90 40-K5/K7	Low	No action required. Affected certificates are in the Java keystore but are not used.
Wireless Gateway exivo 90 42-K7	Low	No action required. No realistic attack scenario exists.
Periphery Connector (PeCo) 92 32-K5, 90 42-K5	Low	No action required. No realistic attack scenario exists.
B-Client AC30-K7	Low	Only use certificates from a trustworthy CA for your host system and access managers. If your certificates were issued by eMudhra, replace them and transfer the root certificate of the new CA to your access managers.
Terminals 96 00-K7/ 98 00-K7	Low	Only relevant for configurations that use a WebView app as part of their application. Optional measure: deactivate the eMudhra credentials in the Android system settings (see Mitigation Details).

Customers operating separate Java-based applications or infrastructure should update Java to the latest version available for their release line, as described in the Oracle Security Alerts CVE-2026-91403 and CVE-2026-114820, or apply the mitigations published by Oracle.

Vulnerability Details

Several intermediate CA certificates issued by eMudhra were compromised and revoked on 18 October 2026. Java does not check certificate revocation by default, so affected Java runtimes continue to trust these certificates until they are updated. An attacker holding a compromised certificate could impersonate any server or peer in TLS connections. Both vulnerabilities can be exploited remotely over the network without authentication or user interaction and have a high impact on confidentiality and integrity, and no impact on availability.

CVE-2026-91403 Compromised eMudhra Intermediate CA Certificates Trusted by Java JSSE

The Java update distrusts eight compromised intermediate CA certificates issued by eMudhra and their cross-signs.

- Classification / Type
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm
  - CWE-284: Improper Access Control
- CVSS Vector:
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
- Base Score: 9.1 (Critical)
- Affected Versions:
  - MATRIX: releases earlier than 4.8 (fix tool available for all maintained releases).
  - B-COMM HCM: All versions earlier than 2026.2.3.
  - B-COMM ERP and B-COMM 7: All versions.
  - resivo Android app: All versions (Android 7.0 and later), through the Android system trust store.
  - Wireless Gateway 90 40-K5/K7: All versions up to and including 5.1.0-109.
  - Wireless Gateway exivo 90 42-K7: All versions up to and including EX.GW-03.01.018-PR.
  - Periphery Connector (PeCo) 92 32-K5, 90 42-K5: All versions up to and including EX.AM-02.05.034-PR.
  - B-Client AC30-K7: All versions up to and including 680-06-X-K02.
  - Terminals 96 00-K7/98 00-K7: All versions up to and including 739-01-X-K04.

CVE-2026-114820 Compromised eMudhra and Sectigo Root CA Certificates in the Java Trust Store

This follow-up fix removes the affected eMudhra and Sectigo root CA certificates from the Java trust store.

- Classification / Type
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm
  - CWE-284: Improper Access Control
- CVSS Vector:
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
- Base Score: 9.1 (Critical)
- Affected Versions:
  - MATRIX: releases earlier than 4.8 (fix tool available for all maintained releases).
  - B-COMM HCM: All versions earlier than 2026.2.3.
  - B-COMM ERP and B-COMM 7: All versions.
  - resivo Android app: All versions (Android 7.0 and later), through the Android system trust store.
  - Wireless Gateway 90 40-K5/K7: All versions up to and including 5.1.0-109.
  - Wireless Gateway exivo 90 42-K7: All versions up to and including EX.GW-03.01.018-PR.
  - Periphery Connector (PeCo) 92 32-K5, 90 42-K5: All versions up to and including EX.AM-02.05.034-PR.
  - B-Client AC30-K7: All versions up to and including 680-06-X-K02.
  - Terminals 96 00-K7/98 00-K7: All versions up to and including 739-01-X-K04.

Mitigation Details (CVE-2026-91403 and CVE-2026-114820)

- MATRIX:

  MATRIX is affected through the certificates in its bundled Java runtime. The fixed Java runtime (Temurin JRE 17.0.21+9) no longer contains the eMudhra root CA certificates. It is delivered with updates of the respective release line: release 4.8 already contains the fix, the update for release 4.7 is planned for approximately 17 November 2026, and the update for release 4.6 will be version 4.6.8 (delivery date not yet known). The date for release 4.5 will be announced. Alternatively, customers can run the executable fix tool. It finds the affected certificate store and removes the eMudhra certificates, performing the same steps as the JRE fix.
  MATRIX Cloud has already been fixed.

- B-COMM HCM:

  B-COMM HCM is affected when it is connected to other systems, for example to dormakaba exos, SAP SuccessFactors or Microsoft Dynamics AX. As an immediate measure, customers should run the script provided by dormakaba. It removes the affected certificates from the Java trust store and adds them to the list of blocked certificates. Version 2026.2.3 (planned for 28 November 2026) performs the same steps during installation. The Java runtime itself will be updated with the next main release 2027.1. Customers should install version 2026.2.3 once it is available.

- B-COMM 7:

  There will be no further releases of B-COMM 7. dormakaba provides a script that removes the affected certificates from the Java trust store and adds them to the list of blocked certificates. Customers should run this script as soon as possible.

- B-COMM ERP:

  B-COMM ERP systems are affected when they are connected, for example, to dormakaba exos (HTTPS only) or Microsoft Dynamics AX. There will be no further releases. dormakaba provides a script that removes the affected certificates from the Java trust store and adds them to the list of blocked certificates. Customers should run this script as soon as possible.

- resivo:

  The resivo cloud services and web apps are not affected. iOS blocks the compromised certificates automatically. The resivo Android app is affected through the Android system trust store. Because the app does not use certificate pinning, an attacker with a compromised eMudhra key and a man-in-the-middle position, for example in a public Wi-Fi network, could read or change app traffic, including login tokens, on devices that still trust the eMudhra root certificates. Customers should keep their Android devices up to date. Optionally, the eMudhra (emSign) certificates can be deactivated in the Android trusted credentials settings, for example under Settings > Security > Trusted credentials > System; the exact menu path depends on the device.

- Wireless Gateway 90 40-K5/K7:

  The affected certificates are contained in the Java trust store of the gateway. However, the gateway has no function that establishes a connection to a trusted server, so the vulnerabilities cannot be exploited in this way. The risk is low. No customer action is required.

- Wireless Gateway exivo 90 42-K7 and Periphery Connector (PeCo) 92 32-K5, 90 42-K5:

  The only external connection these devices establish is to the dormakaba IoT cloud services (exivo/resivo). An attacker holding a compromised eMudhra certificate could impersonate the cloud service, and the device would connect. However, all messages within this connection are additionally encrypted with separately created certificates. The attacker can therefore neither read the messages nor send trusted requests. No realistic attack scenario exists and the risk is low. No customer action is required.

- B-Client AC30-K7:

  AC30 verifies digital certificates issued by the host system. Customers transfer the required root certificates into the access managers themselves, and dormakaba works with user-defined certificates. The vulnerabilities are therefore only relevant if eMudhra certificate authorities are used. Customers are responsible for the certificates they trust and should only use reliable certificates. If host-system certificates were issued by eMudhra, customers should replace them with certificates from a trustworthy CA and transfer the root certificate of the new CA to their access managers.

- Terminals 96 00-K7/97 00-K7:

  The terminals are affected because the Android trust store contains compromised eMudhra certificates. The vulnerabilities are only relevant for configurations that use a WebView app as part of their application and connect to internet-hosted servers. Such a server could be compromised or manipulated in a man-in-the-middle attack but would still be trusted by the system, because of the certificates in the trust store. As an optional measure, customers can deactivate the compromised certificates: open the Android system settings, navigate to Security > Encryption & credentials > Trusted credentials and deactivate the eMudhra credentials.

Additional Information

Legal Disclaimer

Please ensure that your security measures comply with relevant regulatory requirements, including privacy and notification obligations.

Terms of Use

This content is licensed under the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/). If you distribute this content, or a modified version of it, you must provide attribution to dormakaba and provide a link to the original.

Additional Resources

- https://dormakabagroup.com/en/security
- product.security@dormakaba.com

Appendix

CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system, as published by the vendor (Oracle). The base score should be supplemented with an analysis of the affected environment (i.e., Environmental Metrics).

The CVSS scores defined in this advisory are intended to measure the severity of specific vulnerabilities and should not be used alone to assess risk.

Severity	A qualitative measure of a vulnerability within the scope of a specific system.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST SP 800-30).

Estimated Risk Scores

dormakaba qualifies identified vulnerabilities using the OWASP Risk Rating Matrix, assessing likelihood and impact to ensure a consistent, transparent, and business-relevant severity classification based on the system's standard configuration and a "typical" user's environment. This approach supports dormakaba's responsible disclosure process by communicating an estimated risk and remediation prioritization to stakeholders.