# Imprivata EAM Security Advisory: Critical Vulnerabilities Identified and Fixed by Imprivata

| | |
|---|---|
| **Affected Products:** | Imprivata Enterprise Access Management (EAM) |
| **Affected Versions:** | All versions of EAM |
| **Fixed Versions:** | All supported versions of EAM (24.2 – 26.1) |
| **Severity:** | Ranging from Critical to High |

## Partner communication

Dear Valued Partner,

This communication is to inform you about important security updates for Imprivata Enterprise Access Management (EAM) and the guidance Imprivata is providing for your organization and customers to remediate.

The rapid emergence of AI-enabled cyber threats gives bad actors the ability to identify and exploit vulnerabilities with unprecedented speed, scale, and precision. In response to this changing environment, Imprivata has accelerated the pace and rigor of our security reviews, hardening efforts, and architectural guidance updates across our products and services.

Imprivata's latest security review has uncovered potential vulnerabilities (listed in the Summary section below) affecting Imprivata appliances, which, if exploited, could put Imprivata customers at risk.

**While Imprivata has no evidence of exploitation at this time, Imprivata has proactively developed a remediation to these vulnerabilities for supported versions of EAM. Imprivata strongly encourages customers to implement this remediation immediately.**

Below is the full communication that was issued to all customers today. It includes the details of Imprivata's findings, the resolution, and additional steps/resources available to you if necessary.

Imprivata will also host a virtual information session to review the findings and the remediations, and to answer any additional questions you and/or customers may have. The session will take place on Tuesday, June 16 at 10 a.m. ET. Register at: https://security.imprivata.com/eam-security-advisory-update-0616-wb-registration.html.

Please reach out to your Imprivata partner manager with any questions and thank you for your continued partnership.

Sincerely,

Joel Burleson-Davis

Chief Technology and Security Officer

## Full customer communication

Dear Valued Customer,

The rapid emergence of AI-enabled cyber threats gives bad actors the ability to identify and exploit vulnerabilities with unprecedented speed, scale, and precision. In response to this changing environment, Imprivata has accelerated the pace and rigor of our security reviews, hardening efforts, and architectural guidance updates across our products and services.

Imprivata's latest security review has uncovered potential vulnerabilities (listed in the Summary section below) affecting Imprivata appliances, which, if exploited, could put your organization at risk. Below are the details of Imprivata's findings, the recommended steps to resolution, and additional resources.

**While Imprivata has no evidence of exploitation at this time, Imprivata has proactively developed remediation for these vulnerabilities for supported versions of Imprivata Enterprise Access Management (EAM). Imprivata strongly encourages you to implement this remediation immediately.**

Imprivata will host a virtual information session to review the findings and the remediations, and to answer any additional questions you may have. The session will take place on Tuesday, June 16 at 10 a.m. ET. Register at: https://security.imprivata.com/eam-security-advisory-update-0616-wb-registration.html.

As Imprivata continues to use AI-assisted analysis to identify, assess, and resolve emerging risks more quickly, we will continue to communicate an appropriate level of security guidance, remediation recommendations, and hardening activities. Thank you for your continued partnership through these unprecedented times.

**If others within your organization are responsible for vulnerability management, system administration and/or security operations, please share this communication with them to ensure the recommended actions are reviewed and implemented as quickly as possible.**

Sincerely,

Joel Burleson-Davis

Chief Technology and Security Officer

## Summary

Imprivata has identified multiple potential vulnerabilities affecting Imprivata EAM appliances. In response, Imprivata has developed a remediation for supported versions of EAM (24.2 - 26.1). Customers running a version lower than 24.2 will need to upgrade to be able to apply the security fixes. Several of these vulnerabilities are rated Critical and, under certain conditions, could allow unauthenticated or privileged exploitation of appliance components. Therefore, Imprivata **strongly encourages you to implement the applicable hotfix immediately to minimize risk**.

- At this time, Imprivata has no evidence that any of these vulnerabilities have been exploited.
- These vulnerabilities impact **appliances only** and do not affect EAM client software.
- Hotfixes are available for supported versions of EAM (24.2 - 26.1). The hotfixes are currently available through the Imprivata customer portal and can be accessed and implemented through the standard process.
- Please ensure that your organization is using an Imprivata-supported version of EAM. A list of supported versions can be found in our Product Lifecycle Matrix, available on the Imprivata Environment Reference website: https://docs.imprivata.com/supported/content/help.html.
- If you are not running a supported version, you must upgrade to a supported version before deploying a security fix. This includes upgrading to a G4 appliance if you are still using an older version of the appliance. For details and guidance on upgrading, please visit: https://docs.imprivata.com/upgrade/content/topics/upgrade.html.

| Issue ID(s) | Vulnerability Type | Severity (CVSS v3.1) | High-Level Description | Affected Component |
|---|---|---|---|---|
| SCOR-2435, SCOR-2436 | Unauthorized Access | Critical: 9.8 | A vulnerability in the appliance configuration wizard workflow could allow unauthorized access to the appliance from the same network under limited deployment conditions. | Appliance web interface |
| SCOR-2446, SCOR-2447 | Insecure Deserialization | Critical: 9.8 | Improper handling of serialized application data could permit unintended code execution on affected appliances. | Appliance services |
| SCOR-2445 | Authentication Validation Weakness | Critical: 9.1 | An authentication validation issue that affects SAML integrations under specific configurations. | SAML authentication integration |
| SCOR-2442 | Sensitive Data Exposure | High: 8.5 | Sensitive data could be written to the appliance logs under certain circumstances. Interim mitigation for customers who cannot immediately upgrade: Review log forwarding, support bundle, and backup configurations. Assess whether appliance logs have been collected or transmitted externally and apply appropriate access controls to those repositories. | Appliance logging components |
| SCOR-2431 | Credential Management Weakness | High: 8.1 | A credential handling issue could increase risk under specific operational or administrative access conditions. | Appliance platform components |
| SCOR-2443 | Signature Verification Weakness | High: 8.1 | A package verification weakness could reduce the effectiveness of software authenticity validation controls. | Appliance update verification |
| SCOR-2448 | Cryptographic Weakness | High: 7.4 | A weakness in cryptographic validation processes could reduce the integrity assurances of software package validation workflows. | Appliance package validation |
| SCOR-2444 | SQL Injection | High: 7.2 | Insufficient input validation within one of the administrator console functions could allow unintended database interactions by authenticated administrators. Interim mitigation: Audit active administrator accounts; remove admin access from accounts that do not require it. Enable audit logging for admin console activity. | Administrator Console |

## Resolution/Remediation

The vulnerabilities described in this advisory have been remediated via hotfixes for supported versions of EAM. The hotfixes are currently available through the Imprivata customer portal.

Imprivata understands that you may have operational, change-control, and/or other processes preventing your ability to immediately deploy the applicable remediation. If this is the case, Imprivata recommends implementing the following steps to reduce exposure, but please note they **do not fully remediate the vulnerabilities described in this advisory** (applying the hotfix is the only way to do so):

1. **Restrict Network Access to the Appliance**
   Limit inbound access to port 443 (HTTPS) to networks where EAM agents and authorized administrators operate. You should immediately remove direct internet exposure or broad internal network accessibility to appliance interfaces wherever present.
2. **Protect Appliances During Initial Setup**
   Appliances undergoing initial configuration or setup should remain isolated on restricted network segments until setup is complete and the appliance is fully configured according to Imprivata deployment guidance.
3. **Enforce Administrative Console Access Controls**
   Administrative console access should be restricted to authorized personnel operating from approved management workstations. You should review and audit current administrative account assignments and remove unnecessary privileged access.
4. **Review Log and Support Bundle Access Controls**
   If you are using centralized logging, support bundle collection, or backup retention workflows, you should restrict access to EAM log repositories and related data stores to authorized personnel only.

## Customer call to action

- Prioritize the immediate deployment of the hotfix that corresponds to the current version(s) of EAM that you are running, according to internal change-control procedures.
- If you are unable to apply the hotfix at this time, please follow the steps listed in the Resolution/Remediation section above.
- Please register for our virtual session on Tuesday, June 16 at 10 a.m. ET where we will provide more information and answer questions. Register at: https://security.imprivata.com/eam-security-advisory-update-0616-wb-registration.html.
- If you are not running a supported version, you must upgrade to a supported version before deploying a security fix. This includes upgrading to a G4 appliance if you are still using an older version of the appliance. For details and guidance on upgrading, please visit: https://docs.imprivata.com/upgrade/content/topics/upgrade.html.

## Resources

For additional resources on best practices and recommendations for your Imprivata operating environment, please visit the Imprivata Environment Reference website:

https://docs.imprivata.com/supported/content/help.html. Resources available include:

- List of supported EAM versions, available in the Product Lifecycle Matrix on the Imprivata Environment Reference website: https://docs.imprivata.com/supported/content/help.html
- Imprivata EAM Environment Architecture Best Practices guide: https://docs.imprivata.com/supported/content/topics/security/bestpractices_architecture.html
- Guidance for enabling outbound communication for your appliances (to help improve visibility into your EAM environment and allow Imprivata to streamline updates, diagnostics, and support when needed): https://docs.imprivata.com/onesign/content/topics/imprivataplatform/appliance/outboundcomm.html?Highlight=insight

## Imprivata disclaimer

Imprivata assumes no liability for security, performance, or other issues or damages of any kind arising from or related to a customer's failure to install or implement the provided update, patch, or fix. Customers are solely responsible for installing or implementing such provided update, patch, or fix and agree that failure to install or implement such update, patch, or fix may result in security vulnerabilities or degradation of performance for which Imprivata is not responsible.

If you have any questions or would like additional information, please visit the Imprivata Customer Experience Center.