Unauthenticated SSRF via PENS Plugin allows attacker to probe internal network and reach cloud metadata services (<=2.0-RC.2)

High **ywarnier** published **GHSA-g2xj-4cch-j276** 9 hours ago

Package

chamilo/chamilo-lms (PHP)

Affected versions	Patched versions
2.0-RC.2	2.0-RC.3

Description

Summary

The PENS (Package Exchange Notification Services) plugin endpoint at `public/plugin/Pens/pens.php` in Chamilo LMS 2.x (latest master, commit `af6b7002af7c15825e98fc522e2ead0d00cacaa3`) is accessible without authentication and accepts a user-controlled `package-url` parameter. The server fetches this URL using curl without filtering private/internal IP addresses, enabling unauthenticated Server-Side Request Forgery (SSRF) to internal network services and cloud metadata endpoints.

Impact

1. **Internal Network Reconnaissance**: An unauthenticated attacker can use the PENS endpoint to probe internal network services (databases, admin panels, internal APIs) by observing response timing and error messages.
2. **Cloud Metadata Access**: In cloud environments (AWS, GCP, Azure), an attacker can reach the instance metadata service at `169.254.169.254` to steal IAM credentials, instance identity tokens, and other sensitive metadata. This can lead to full cloud account compromise.

3. **Callback SSRF for Internal Service Interaction**: The `receipt` and `alerts` parameters cause the server to make POST requests to attacker-specified internal URLs, potentially triggering state-changing operations on internal services.

4. **Unauthenticated Access**: No authentication is required to exploit either SSRF vector, increasing the attack surface significantly.

Fix

`de4058d`

Severity

High 8.6 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

CVE ID

CVE-2026-34160

Weaknesses

- CWE-306
- CWE-918

Credits

romain-deperne Reporter