Unauthenticated SSRF and Open Email Relay via install.ajax.php test_mailer action (<=2.0-RC.2)

High **ywarnier** published **GHSA-mxc9-9335-45mc** 9 hours ago

Package

chamilo/chamilo-lms (PHP)

Affected versions

2.0-RC.2

Patched versions

2.0-RC.3

Description

Summary

The file `public/main/inc/ajax/install.ajax.php` is accessible without authentication on fully installed Chamilo LMS 2.0 instances. Its `test_mailer` action accepts an arbitrary Symfony Mailer DSN string from POST data and uses it to connect to an attacker-specified SMTP server and send an email to an attacker-specified destination. This enables Server-Side Request Forgery (SSRF) into internal networks via SMTP protocol and can be abused as an open email relay for phishing and spam campaigns.

Details

The vulnerability exists because `install.ajax.php` was designed for the installation wizard but remains accessible after installation. Unlike other AJAX endpoints in the same directory, this file does **not** include `global.inc.php` (which performs authentication and installation-completed checks). It only loads the Composer autoloader:

Impact

1. **Server-Side Request Forgery (SSRF)**: An unauthenticated attacker can force the Chamilo server to initiate SMTP connections to arbitrary internal or external hosts, enabling internal network reconnaissance and potential exploitation of internal mail servers.

2. **Open Email Relay**: The Chamilo server can be weaponized as an open email relay. Attackers can send phishing emails or spam through the server, with the emails appearing to originate from the Chamilo server's IP address. This can damage the organization's email reputation and domain trust.

3. **Information Disclosure**: Error responses from failed SMTP connections may reveal information about the internal network topology, running services, and firewall rules.

Severity

High 7.2 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-33715

Weaknesses

- CWE-306
- CWE-918

Credits

romain-deperne Reporter