EspoCRM: SSRF via DNS Rebinding in Attachment fromImageUrl Endpoint Allows Internal Network Access

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-33659
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 21:16:24 UTC
Updated	2026-04-13 21:16:24 UTC
Description	EspoCRM is an open source customer relationship management application. In versions 9.3.3 and below, the POST /api/v1

Risk And Classification

Primary CVSS: v3.1 3.5 LOW from security-advisories@github.com

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

Problem Types: CWE-367 | CWE-918 | CWE-918 CWE-918: Server-Side Request Forgery (SSRF) | CWE-367 CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	3.5	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N
3.1	CNA	DECLARED	3.5	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Espocrm	Espocrm	affected < 9.3.4	Not specified

References

Reference	Source	Link	T
github.com/espocrm/espocrm/security/advisories/GHSA-6m4j-fwrx-crh7	security-advisories@github.com	github.com	
github.com/espocrm/espocrm/commit/dca03cc3458e487362c26c746378a2d4de9990b1	security-advisories@github.com	github.com	
github.com/espocrm/espocrm/releases/tag/9.3.4	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.