monetr is vulnerable to server-side request forgery in Lunch Flow link creation and refresh

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

Summary

CVE	CVE-2026-41644
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 12:16:17 UTC
Updated	2026-05-11 16:40:30 UTC
Description	monetr is a budgeting application for recurring expenses. Prior to version 1.12.5, a server-side request forgery (SSRF) vuln

Risk And Classification

Primary CVSS: v4.0 8.3 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:L/SC:H/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000390000 probability, percentile 0.116770000 (date 2026-05-12)

Problem Types: CWE-209 | CWE-770 | CWE-918 | CWE-209 CWE-209: Generation of Error Message Containing Sensitive Information | CWE-770 CWE-770: Allocation of Resources Without Limits or Throttling | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.3	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:L/SC:H/S
4.0	CNA	DECLARED	8.3	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:L/SC:H/S
3.1	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

None

Availability

Low

Sub Conf.

High

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:L/SC:H/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Monetr	Monetr	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Monetr	Monetr	affected < 1.12.5	Not specified

References

Reference	Source	Link	Tag
github.com/monetr/monetr/security/advisories/GHSA-29v9-frvh-c426	security-advisories@github.com	github.com	Mitig
github.com/monetr/monetr/pull/3122	security-advisories@github.com	github.com	Issu
github.com/monetr/monetr/releases/tag/v1.12.5	security-advisories@github.com	github.com	Proc
github.com/monetr/monetr/commit/c260caa3c573a4a396ec2d264c7641a5d958385b	security-advisories@github.com	github.com	Patc
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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