Squidex has Blind SSRF via file:// Protocol in Restore API leading to Local File Interaction

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

Summary

CVE	CVE-2026-41177
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 22:16:31 UTC
Updated	2026-04-22 22:16:31 UTC
Description	Squidex is an open source headless content management system and content management hub. Prior to version 7.23.0, th

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from security-advisories@github.com

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

Problem Types: CWE-73 | CWE-918 | CWE-73 CWE-73: External Control of File Name or Path | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:L
3.1	CNA	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

Integrity

None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Squidex	Squidex	affected < 7.23.0	Not specified

References

Reference	Source	Link	Ta
github.com/Squidex/squidex/commit/b81d75e1d9c1a8e30993c2ee59b350002b9aeda4	security-advisories@github.com	github.com	
github.com/Squidex/squidex/security/advisories/GHSA-45fq-w37p-qfw5	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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