Arbitrary File Read and Server Side Request Forgery via XML External Entities in Lobster_pro

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

Summary

CVE	CVE-2024-13971
State	PUBLISHED
Assigner	SCHUTZWERK
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 13:16:02 UTC
Updated	2026-05-17 23:17:01 UTC
Description	Unauthenticated attackers can exploit a weakness in the XML parser functionality of Lobster_pro prior to version 4.12.6-GA

Risk And Classification

Primary CVSS: v4.0 7.7 HIGH from 23637b5d-af4c-4cf9-b8f6-deb7fd0f8423

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/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:N/AU:Y/R:X/V:C/RE:X/U:X

EPSS: 0.000200000 probability, percentile 0.056620000 (date 2026-05-17)

Problem Types: CWE-611 | CWE-611 CWE-611 Improper Restriction of XML External Entity Reference

Version	Source	Type	Score	Severity	Vector
4.0	23637b5d-af4c-4cf9-b8f6-deb7fd0f8423	Secondary	7.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/S
4.0	CNA	CVSS	7.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/S
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/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:N/AU:Y/R:X/V:C/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lobster-world	Lobster Pro	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Lobster GmbH	Lobster Pro	affected 4.12.6-GA custom	Windows
CNA	Lobster GmbH	Lobster Pro	unaffected 4.12.6-GA custom	Windows

References

Reference	Source	Link	Tags
seclists.org/fulldisclosure/2026/May/1	af854a3a-2127-422b-91ae-364da2661108	seclists.org	
www.schutzwerk.com/en/blog/schutzwerk-sa-2024-005	23637b5d-af4c-4cf9-b8f6-deb7fd0f8423	www.schutzwerk.com	Exploit, Third F
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

Vendor Comments And Credit

Discovery Credit

CNA: Marcelo Reyes of SCHUTZWERK GmbH (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-08-12T11:00:00.000Z	Initial contact with vendor
CNA	2024-08-14T11:00:00.000Z	Vulnerability reported to vendor
CNA	2024-08-14T11:00:00.000Z	CVE ID requested
CNA	2024-08-22T11:00:00.000Z	Initial feedback received from vendor: unable to reproduce
CNA	2024-08-28T11:00:00.000Z	Vulnerability demonstrated in vendor's "Community server"
CNA	2024-09-19T11:00:00.000Z	Vulnerability reported fixed by vendor in Lobster_pro release 4.12.6-GA
CNA	2025-07-03T11:00:00.000Z	Reserved CVE ID CVE-2024-13971
CNA	2026-04-30T11:00:00.000Z	Advisory released

Solutions

CNA: Update to Lobster_pro release 4.12.6-GA or higher.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**