Server-Side Request Forgery in API Checker leads to Privilege Escalation

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

Summary

CVE	CVE-2026-30810
State	PUBLISHED
Assigner	PandoraFMS
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 16:16:13 UTC
Updated	2026-05-12 16:47:47 UTC
Description	Server-Side Request Forgery vulnerability allows Privilege Escalation via API Checker extension. This issue affects Pandor

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from security@pandorafms.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/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:U/V:C/RE:M/U:Amber

Problem Types: CWE-918 | CWE-918 CWE-918 Server-Side request forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	security@pandorafms.com	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:N
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

ntegrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/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:U/V:C/RE:M/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pandora FMS	Pandora FMS	affected 777 800 custom	all

References

Reference	Source	Link	Tags
pandorafms.com/en/security/common-vulnerabilities-and-exposures	security@pandorafms.com	pandorafms.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Pedro J. Núñez-Cacho Fuentes <tunelko@gmail.com> (en)

Additional Advisory Data

Solutions

CNA: Fixed in v802 and v800.2

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**