



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

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

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

## 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/MSX/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

Integrity

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/MSX: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	<a href="#">Pandora FMS</a>	<a href="#">Pandora FMS</a>	affected 777 800 custom	all

### References

Reference	Source	Link	Tags
<a href="#">pandorafms.com/en/security/common-vulnerabilities-and-exposures</a>	<a href="mailto:security@pandorafms.com">security@pandorafms.com</a>	<a href="#">pandorafms.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Pedro J. Núñez-Cacho Fuentes <[tunnelko@gmail.com](mailto:tunnelko@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.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)