



# Missing Authorization in Configuration Ajax Endpoint leads to Information Disclosure

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

## Summary

<b>CVE</b>	CVE-2026-30811
<b>State</b>	PUBLISHED
<b>Assigner</b>	PandoraFMS
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-13 16:16:25 UTC
<b>Updated</b>	2026-04-22 14:31:22 UTC
<b>Description</b>	Missing Authorization vulnerability allows Exposure of Sensitive Information via configuration endpoint. This issue affects P

## Risk And Classification

**Primary CVSS:** v4.0 8.4 HIGH from security@pandorafms.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:H/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:L/U:Amber

**EPSS:** 0.000430000 probability, percentile 0.132270000 (date 2026-04-22)

**Problem Types:** CWE-276 | CWE-276 CWE-276 Incorrect default permissions

Version	Source	Type	Score	Severity	Vector
4.0	security@pandorafms.com	Secondary	8.4	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:
4.0	CNA	CVSS	8.4	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/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

Low

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

High

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

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/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	Artica	Pandora Fms	All	All	All	All

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

## Vendor Comments And Credit

### Discovery Credit

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

## Additional Advisory Data

### Solutions

**CNA:** Fixed in v800.1 and v801 Pandora FMS versions

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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)