Missing Authorization in Configuration Ajax Endpoint leads to Information Disclosure

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

Summary

CVE	CVE-2026-30811
State	PUBLISHED
Assigner	PandoraFMS
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 16:16:25 UTC
Updated	2026-04-22 14:31:22 UTC
Description	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/MSC:X/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/MSC: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	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	Vendor Advisory
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 v800.1 and v801 Pandora FMS versions

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