Insecure Default Initialization in API Authentication leads to Authentication Bypass

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

Summary

CVE	CVE-2026-30805
State	PUBLISHED
Assigner	PandoraFMS
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 16:16:12 UTC
Updated	2026-05-12 16:47:47 UTC
Description	Insecure Default Initialization of Resource vulnerability allows Authentication Bypass via API access. This issue affects Pan

Risk And Classification

Primary CVSS: v4.0 9.1 CRITICAL from security@pandorafms.com

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

Problem Types: CWE-1188 | CWE-1188 CWE-1188 Initialization of a resource with an insecure default

Version	Source	Type	Score	Severity	Vector
4.0	security@pandorafms.com	Secondary	9.1	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S
4.0	CNA	CVSS	9.1	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/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:N/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 800.2

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