# Session Fixation in Authentication leads to Session Hijacking

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-30808 |
| **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** | Session Fixation vulnerability allows Session Hijacking via crafted session ID. This issue affects Pandora FMS: from 777 th |

## Risk And Classification

**Primary CVSS:** v4.0 7.6 HIGH from security@pandorafms.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/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:L/U:Amber

**Problem Types:** CWE-384 | CWE-384 CWE-384 Session fixation

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | security@pandorafms.com | Secondary | 7.6 | HIGH | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA |
| 4.0 | CNA | CVSS | 7.6 | HIGH | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

High

ntegrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/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:L/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.

© 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 registred 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

**CVE.report and Source URL Uptime Status** **status.cve.report**