



CVE-2020-11749

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

Summary

CVE	CVE-2020-11749
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-13 15:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	Pandora FMS 7.0 NG <= 746 suffers from Multiple XSS vulnerabilities in different browser views. A network administrator s

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pandorafms	Pandora Fms	All	All	All	All

References

Reference	Source	Link	Tags
Multiple XSS on PandoraFMS 7.0 NG 744 - AppleBois - Medium	MISC	medium.com	Exploit, Third Pa
Pandora FMS 7.0 NG 746 Script Insertion / Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Pa
PandoraFMS 7.0 NG 746 - Persistent Cross-Site Scripting - PHP webapps Exploit	MISC	www.exploit-db.com	
pandorafms.com/downloads/whats-new-747-EN.pdf	CONFIRM	pandorafms.com	Release Notes, '
CVE 2020–11749. We all know XSS is dangerous... by AppleBois Medium		medium.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)