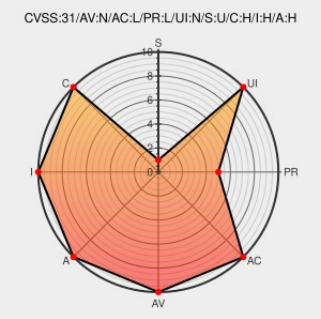
CVE-2019-20224

Published on: 01/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:50 PM UTC

CVE-2019-20224

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pandora Fms from Artica contain the following vulnerability:

netflow_get_stats in functions_netflow.php in Pandora FMS 7.0NG allows remote authenticated users to execute arbitrary OS commands via shell metacharacters in the ip_src parameter in an index.php?operation/netflow/nf_live_view request. This issue has been fixed in Pandora FMS 7.0 NG 742.

CVE-2019-20224 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
	pandorafms.com video/mp4	MISC pandorafms.com/downloads/solved-pandorafms-742.mp4
PandoraFMS v7.0NG authenticated Remote	Exploit	MISC shells.systems/pandorafms-v7-0ng-authenticated-

Code Execution (CVE-2019-20224) - Shells.Systems	Exploit Third Party Advisory shells.systems text/html	remote-code-execution-cve-2019-20224/
Pandora 7.0NG Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155897/Pandora-7.0NG-Remote-Code-Execution.html
Pandora-PostAuth-2019-11-14_21.34.54.mp4 - Google Drive	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC drive.google.com/file/d/1DkWR5MylzeNr20jmHXTaAIJmf3YN-InO/view?usp=sharing
Pandora-exploit.py · GitHub	Exploit Third Party Advisory gist.github.com text/html	MISC gist.github.com/mhaskar/2153d66a0928492d76b799ba13b9e3f9

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

The offical exploit for Pandora v7.0NG Post-auth Remote Code Execution CVE-2019-20224

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Artica	Pandora Fms	7.0_ng	All	All	All
Application	Artica	Pandora Fms	7.0_ng	All	All	All

cpe:2.3:a:artica:pandora_fms:7.0_ng:*:*:*:*:*:*:*:

cpe:2.3:a:artica:pandora_fms:7.0_ng:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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