



# CVE-2020-5844

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

## Summary

|                        |                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2020-5844                                                                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                                                                    |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                                                             |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                                                              |
| <b>Published</b>       | 2020-03-16 18:15:00 UTC                                                                                                                                                   |
| <b>Updated</b>         | 2022-11-29 16:57:00 UTC                                                                                                                                                   |
| <b>Description</b>     | index.php?sec=godmode/extensions&sec2=extensions/files_repo in Pandora FMS v7.0 NG allows authenticated administrators to execute arbitrary code via the 'sec' parameter. |

## Risk And Classification

### Problem Types: CWE-434

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                     | Version | Update | Edition | Language |
|-------------|------------------------|-----------------------------|---------|--------|---------|----------|
| Application | <a href="#">Artica</a> | <a href="#">Pandora Fms</a> | 7.0_ng  | All    | All     | All      |
| Application | <a href="#">Artica</a> | <a href="#">Pandora Fms</a> | 7.0_ng  | All    | All     | All      |

## References

| Reference                                                  | Source  | Link                                    | Tags                          |
|------------------------------------------------------------|---------|-----------------------------------------|-------------------------------|
| Pandora FMS 7.0NG.742 Remote Code Execution ~ Packet Storm | MISC    | <a href="#">packetstormsecurity.com</a> |                               |
| Pandora FMS - the Flexible Monitoring System               | MISC    | <a href="#">pandorafms.com</a>          | Product                       |
| GitHub - TheCyberGeek/CVE-2020-5844                        | MISC    | <a href="#">github.com</a>              | Exploit, Third Party Advisory |
| CVE Program record                                         | CVE.ORG | <a href="#">www.cve.org</a>             | canonical                     |
| NVD vulnerability detail                                   | NVD     | <a href="#">nvd.nist.gov</a>            | canonical, analysis           |

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)