



CVE-2023-43872

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-43872 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-09-28 14:15:00 UTC |
| Updated | 2023-10-30 19:45:00 UTC |
| Description | A File upload vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to upload a pdf file with hidden Cross Site Sc |

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-------------------------------|---------------------------------|---------|--------|---------|----------|
| Application | Cmsmadesimple | Cmsmadesimple | 2.2.18 | All | All | All |
| Application | Cmsmadesimple | Cms Made Simple | 2.2.18 | All | All | All |

References

Reference

GitHub - sromanhu/CMSmadesimple-File-Upload--XSS---File-Manager: CMSmadesimple 2.2.18 is affected by File Upload - XSS vulnerability

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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