



CVE-2018-18548

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

Summary

CVE	CVE-2018-18548
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-24 21:29:00 UTC
Updated	2018-12-06 20:23:00 UTC
Description	ajenticp (aka Ajenti Docker control panel) for Ajenti through v1.2.23.13 has XSS via a filename that is mishandled in File M...

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ajenti	Ajenticp	All	All	All	All

References

Reference	Source	Link	Tags
AjentiCP 1.2.23.13 - Cross-Site Scripting - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com	Third Party Advisory, VDB Entr
numanozdemir.com/ajenti-xss.txt	MISC	numanozdemir.com	Third Party Advisory
AjentiCP 1.2.23.13 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party Advisory, VDB Entr
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#).

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