



CVE-2018-13983

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

Summary

CVE	CVE-2018-13983
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-06 19:29:00 UTC
Updated	2019-05-07 12:24:00 UTC
Description	ImpressCMS 1.3.10 has XSS via the PATH_INFO to htdocs/install/index.php, htdocs/install/page_langselect.php, or htdocs

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Impresscms	Impresscms	1.3.10	All	All	All
Application	Impresscms	Impresscms	1.3.10	All	All	All

References

Reference	Source	Link	Tags
NS-18-033 ImpressCMS vulnerable to Cross-site Scripting Netsparker	MISC	www.netsparker.com	Exploit, Third Pa
Full Disclosure: Multiple Cross-site Scripting Vulnerabilities in ImpressCMS 1.3.10	MISC	seclists.org	Mailing List, Thir
ImpressCMS 1.3.10 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Pa
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.

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](#)