CVE-2018-9844

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-9844
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-07 07:29:00 UTC
Updated	2018-05-11 14:04:00 UTC
Description	The Iptanus WordPress File Upload plugin before 4.3.4 for WordPress mishandles Settings attributes, leading to XSS.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Iptanus	Wordpress File Upload	All	All	All	All
Application	Iptanus	Wordpress File Upload	All	All	All	All

References

Reference	Source	Link	Tags
WordPress Plugin File Upload 4.3.3 - Stored Cross-Site Scripting (PoC) - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com	Expl
New Version 4.3.4 of WordPress File Upload Plugin - Iptanus	CONFIRM	www.iptanus.com	Vend
WordPress File Upload – WordPress plugin | WordPress.org	CONFIRM	wordpress.org	Third
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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