



CVE-2019-6112

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

Summary

CVE	CVE-2019-6112
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-14 14:15:00 UTC
Updated	2020-08-19 15:21:00 UTC
Description	A Cross-site scripting (XSS) vulnerability in /inc/class-search.php in the Sell Media plugin v2.4.1 for WordPress allows remote users to inject arbitrary HTML and JavaScript code into the page. This vulnerability is caused by the lack of output escaping in the search.php file. An attacker can exploit this vulnerability by sending a specially crafted request to the search.php file. The attacker can then inject arbitrary HTML and JavaScript code into the page. This can be used to steal sensitive information, such as cookies and session IDs, and to perform other malicious actions.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Graphpaperpress	Sell Media	All	All	All	All

References

Reference	Source	Link
Fixed masonry layouts, sanitized search input, and misc PHP notices · graphpaperpress/Sell-Media@8ac8ceb · GitHub	CONFIRM	github.
metamorfosec.com/Files/Advisories/METS-2020-001-A_XSS_Vulnerability_in_Sell_Me...	MISC	metar
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

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](#).

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