



CVE-2018-1002001

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

Summary

CVE	CVE-2018-1002001
State	PUBLIC
Assigner	larry0@me.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-03 16:29:00 UTC
Updated	2018-12-27 17:36:00 UTC
Description	There is a reflected XSS vulnerability in WordPress Arigato Autoresponder and News letter v2.5.1.8 This vulnerability requires an authenticated user to be able to exploit it. The vulnerability is located in the wp_arigato_autoresponder.php file, line 100. The vulnerability is a reflected XSS, which means that the attacker can inject malicious code into the page, which will be executed by the browser. This vulnerability can be exploited by sending a request to the WordPress site with a malicious payload in the 'arigato_autoresponder' parameter. The payload will be reflected back in the response, and the browser will execute it. This can lead to the execution of arbitrary code on the server, or the theft of sensitive information.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kibokolabs	Arigato Autoresponder And Newsletter	2.5.1.8	All	All	All
Application	Kibokolabs	Arigato Autoresponder And Newsletter	2.5.1.8	All	All	All

References

Reference	Source
WordPress Plugin Arigato Autoresponder and Newsletter 2.5 - Blind SQL Injection / Reflected Cross-Site Scripting - PHP webapps Exploit	Exploit-DB
Arigato Autoresponder and Newsletter — WordPress Plugins	WordPress.org
Larry Cashdollar Vulnerability	Medium
CVE Program record	CVE
NVD vulnerability detail	NVD

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