



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

CVE	CVE-2018-1002002
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 17:47:00 UTC
Description	There is a reflected XSS vulnerability in WordPress Arigato Autoresponder and News letter v2.5.1.8 This vulnerability requires a user to be logged in to the site and have access to the newsletter settings. An attacker can exploit this vulnerability by sending a specially crafted email to the newsletter settings page. The attacker can then inject arbitrary HTML code into the newsletter template, which will be rendered to all subscribers. This vulnerability can be exploited by sending a specially crafted email to the newsletter settings page. The attacker can then inject arbitrary HTML code into the newsletter template, which will be rendered to all subscribers. This vulnerability can be exploited by sending a specially crafted email to the newsletter settings page. The attacker can then inject arbitrary HTML code into the newsletter template, which will be rendered to all subscribers.

Problem Types: CWE-79

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

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

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