



Mail Control <= 0.2.8 - Unauthenticated Stored Cross-Site Scripting via Email Subject

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2023-3158
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-12 05:15:10 UTC
Updated	2026-04-08 18:18:08 UTC
Description	The Mail Control plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, ar

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Instareza	Mail Control	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	P
CNA	Rahalaboulfeth	Mail Control Email Customizer SMTP Deliverability Logging Open And Click Tracking	affected 0.3.1 semver	N

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.t
Mail Control <= 0.2.8 - Unauthenticated Stored Cross-Site Scripting via Email Subject	af854a3a-2127-422b-91ae-364da2661108	www.wo
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.t
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

Vendor Comments And Credit

Discovery Credit

CNA: Alex Thomas (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-06-07T00:00:00.000Z	Discovered
CNA	2023-06-22T00:00:00.000Z	Vendor Notified
CNA	2023-07-10T00:00:00.000Z	Disclosed

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

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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