



CVE-2022-21179

Published on: Not Yet Published

Last Modified on: 03/03/2022 07:25:00 PM UTC

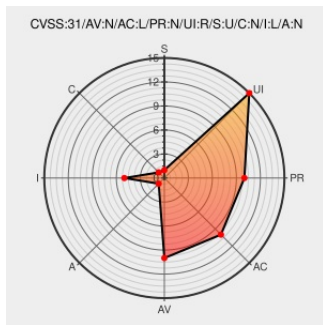
CVE-2022-21179

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [E-mail Newsletter Management](#) from [Ec-cube](#) contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in EC-CUBE plugin 'Mail Magazine Management Plugin' ver4.0.0 to 4.1.1 (for EC-CUBE 4 series) and ver1.0.0 to 1.0.4 (for EC-CUBE 3 series) allows a remote unauthenticated attacker to hijack the authentication of an administrator via a specially crafted page, and Mail Magazine Templates and/or transmitted history information may be deleted unintendedly.

CVE-2022-21179 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [EC-CUBE CO.,LTD.](#) - [EC-CUBE plugin 'Mail Magazine Management Plugin'](#) version **ver4.0.0 to 4.1.1 (for EC-CUBE 4 series) and ver1.0.0 to 1.0.4 (for EC-CUBE 3 series)**

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Type	Link
-------------	------	------

Description	Tags	Link
EC-CUBE メルマガ管理プラグインにおける CSRFの脆弱性	www.ec-cube.net text/html	MISC www.ec-cube.net/info/weakness/20220221/mail_magazine_plugin.php
JVN#67108459: EC-CUBE plugin "Mail Magazine Management Plugin" vulnerable to cross-site request forgery	jvn.jp text/xml	MISC jvn.jp/en/jp/JVN67108459/index.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ec-cube	E-mail Newsletter Management	All	All	All	All
Application	Ec-cube	E-mail Newsletter Management	All	All	All	All

cpe:2.3:a:ec-cube:e-mail_newsletter_management:*:*:*:*:ec-cube:*:*:

cpe:2.3:a:ec-cube:e-mail_newsletter_management:*:*:*:*:ec-cube:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-21179 : Cross-site request forgery CSRF vulnerability in EC-CUBE plugin 'Mail Magazine Management Plugin... twitter.com/i/web/status/1...	2022-02-28 18:44:03

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022 [Twitter](#) [News](#) |

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](#).

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