



CVE-2021-4121

Published on: 12/16/2021 12:00:00 AM UTC

Last Modified on: 12/20/2021 01:35:00 PM UTC

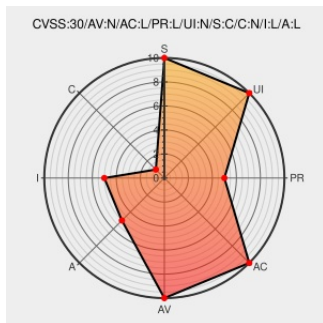
CVE-2021-4121 - advisory for 6da878de-acdb-4b97-b9ff-9674c3f0881d

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **Yetiforce Customer Relationship Management** from **Yetiforce** contain the following vulnerability:

yetiforcecrm is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVE-2021-4121 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: yetiforcecompany - yetiforcecompany/yetiforcecrm version < 6.4.0

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	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	Tags	Link
Improved MeetingUrl uitype - YetiForceCompany/YetiForceCRM@6b59671 - GitHub	github.com text/html	MISC github.com/yetiforcecompany/yetiforcecrm/commit/6b5967198e4

huntr – the Bug Bounty Platform for any
GitHub repository

[huntr.dev](#)

[text/html](#)

Inactive Link

Not Archived

 [CONFIRM huntr.dev/bounties/6da878de-acdb-4b97-b9ff-9674](#)

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	Yetiforce	Yetiforce Customer Relationship Management	All	All	All	All
cpe:2.3:a:yetiforce:yetiforce_customer_relationship_management:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @huntrHacktivity	Cross-site Scripting (XSS) - Stored in github.com/yetiforcecompa... (CVE-2021-4121) reported by laladee - Patch:... twitter.com/i/web/status/1...	2021-12-15 08:01:55
 @CVEreport	CVE-2021-4121 : yetiforcecrm is vulnerable to Improper Neutralization of Input During Web Page Generation 'Cross-s... twitter.com/i/web/status/1...	2021-12-16 07:37:01
 @OpenSourceHacks	(CVE-2021-4121): Cross-site Scripting (XSS) - Stored in yetiforcecompany/yetiforcecrm. Disclosed by... twitter.com/i/web/status/1...	2021-12-16 08:32:26
 /r/netcve	CVE-2021-4121	2021-12-16 08:38:01

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)