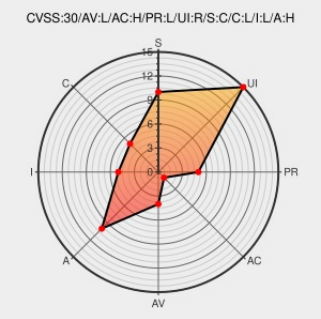
CVE-2021-4116

Published on: 12/15/2021 12:00:00 AM UTC

Last Modified on: 12/17/2021 02:32:00 PM UTC

CVE-2021-4116 - advisory for 7561bae7-9053-4dc8-aa59-b71acfb1712c

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-2021-4116 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: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
Improved validation of uploaded files · YetiForceCompany/YetiForceCRM@9cdb012 · GitHub	github.com text/html	MISC github.com/yetiforcecompany/yetiforcecrm/commit/9cdb012ca64ff1f719f8120d5

Cross-site Scripting (XSS) - Stored vulnerability found in yetiforcecrm	huntr.dev text/html	CONFIRM huntr.dev/bounties/7561bae7-9053-4dc8-aa59-b71acfb1712c

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)
@SystemTek_UK	Advanced Content Filter (ACF) vulnerability allowing to execute JavaScript code using malformed HTML [CVE-2021-4116… twitter.com/i/web/status/1…	2021-11-19 20:50:12
@6townstechteam	Advanced Content Filter (ACF) vulnerability allowing to execute JavaScript code using malformed HTML [CVE-2021-4116… twitter.com/i/web/status/1…	2021-11-19 20:50:13
@OpenSourceHacks	(CVE-2021-4116): Cross-site Scripting (XSS) - Stored in yetiforcecompany/yetiforcecrm. Disclosed by… twitter.com/i/web/status/1…	2021-12-15 14:32:19
@prophaze	CVE-2021-4116 prophaze.com/cve/cve-2021-4…	2021-12-15 23:05:21
@threatmeter	CVE-2021-4116 yetiforcecrm is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-sit… twitter.com/i/web/status/1…	2021-12-15 23:08:52
@prophaze	yetiforcecrm Web Page Generation cross site scripting [CVE-2021-4116] prophaze.com/cve/yetiforcec… #Exploit:No #Local:No… twitter.com/i/web/status/1…	2021-12-16 08:13:48

← Previous ID Next ID→