



CVE-2022-2829

Published on: Not Yet Published

Last Modified on: 08/24/2022 02:26:00 PM UTC

CVE-2022-2829 - advisory for d6eaa453-9758-41b7-8c38-fd878d6aeab4

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Yetiforce Customer Relationship Management](#) from [Yetiforce](#) contain the following vulnerability:

Cross-site Scripting (XSS) - Stored in GitHub repository [yetiforcecompany/yetiforcecrm](#) prior to 6.4.0.

CVE-2022-2829 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

CVE References

Description	Tags	Link
YetiForce CRM ver. 6.4.0 (#16359) · YetiForceCompany/YetiForceCRM@2c14baa · GitHub	github.com text/html	MISC github.com/yetiforcecompany/yetiforcecrm/commit/2c14baaf8dbc7fd82d5c585f2
Stored XSS vulnerability when importing RSS Feeds from external source vulnerability found in yetiforcecrm	huntr.dev text/html	CONFIRM huntr.dev/bounties/d6eaa453-9758-41b7-8c38-fd878d6aeab4

By selecting these links, you may be leaving CVEreport workspace. 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-2022-2829) reported by 0xb4c - Patch:... twitter.com/i/web/status/1...	2022-08-22 07:02:16
 @CVEreport	CVE-2022-2829 : Cross-site Scripting #XSS - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.... twitter.com/i/web/status/1...	2022-08-23 04:05:42
 @threatmeter	CVE-2022-2829 Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0... twitter.com/i/web/status/1...	2022-08-23 23:06:55
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-2829 - Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecomp... twitter.com/i/web/status/1...	2022-08-23 23:07:02
 @threatmeter	CVE-2022-2829 Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0... twitter.com/i/web/status/1...	2022-08-24 07:09:22
 @OpenSourceHacks	(CVE-2022-2829): Cross-site Scripting (XSS) - Stored in yetiforcecompany/yetiforcecrm. huntr.dev/bounties/d6eaa... Di... twitter.com/i/web/status/1...	2022-08-26 03:56:50
 /r/netcve	CVE-2022-2829	2022-08-23 04:38:24

[← 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](#)