



CVE-2021-32853

Published on: Not Yet Published

Last Modified on: 03/06/2023 10:19:52 PM UTC

CVE-2021-32853 - advisory for GHSL-2021-103

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Erxes](#) from [Erxes](#) contain the following vulnerability:

Erxes, an experience operating system (XOS) with a set of plugins, is vulnerable to cross-site scripting in versions 0.22.3 and prior. This results in client-side code execution. The victim must follow a malicious link or be redirected there from malicious web site. There are no known patches.

CVE-2021-32853 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **npm** - **erxes** version **<= 0.22.3**

CVSS3 Score: **9.6 - CRITICAL**

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

CVE References

Description	Tags	Link
erxes/index.ts at f131b49add72032650d483f044d00658908aaf4a · erxes/erxes · GitHub	github.com text/html	MISC github.com/erxes/erxes/blob/f131b49add72032650d483f044d00658908aaf4a/erxes/index.ts
erxes/widget.ejs at f131b49add72032650d483f044d00658908aaf4a · erxes/erxes · GitHub	github.com text/html	MISC github.com/erxes/erxes/blob/f131b49add72032650d483f044d00658908aaf4a/erxes/widget.ejs
GHSL-2021-103: Cross-Site Scripting (XSS) in Erxes - CVE-2021-32853 GitHub Security Lab	securitylab.github.com text/html	CONFIRM securitylab.github.com/advisories/GHSL-2021-103-e

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	Erxes	Erxes	All	All	All	All
cpe:2.3:a:erxes:erxes:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @GHSecurityLab	GHSL-2021-103: Cross-Site Scripting (XSS) in Erxes - CVE-2021-32853 github.co/34vBe60	2022-02-01 17:40:00
 @CVEreport	CVE-2021-32853 : Erxes, an experience operating system XOS with a set of plugins, is vulnerable to cross-site scr... twitter.com/i/web/status/1...	2023-02-20 22:28:24

← 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](#)