



CVE-2021-39221

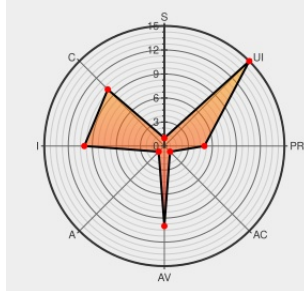
Published on: 10/25/2021 12:00:00 AM UTC

Last Modified on: 10/27/2021 03:09:00 PM UTC

CVE-2021-39221 - advisory for GHSA-j6cx-mxqf-f9vc

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

CVSS:31/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N



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

Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Contacts application prior to version 4.0.3 was vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. For exploitation, a user would need to right-click on a malicious file and open the file in a new tab. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. It is recommended that the Nextcloud Contacts application is upgraded to 4.0.3. As a workaround, one may use a browser that has support for Content-Security-Policy.

CVE-2021-39221 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: nextcloud - security-advisories version < 4.0.3

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

Run SVGs through some sanitization by ChristophWurst · Pull Request #2407 · nextcloud/contacts · GitHub

XSS in Contacts · Advisory · nextcloud/security-advisories · GitHub

Tags

github.com

text/html

github.com

text/html

Link

MISC

github.com/nextcloud/contacts/pull/2407

CONFIRM

github.com/nextcloud/security-advisories/security/advisories/GHSA-j6cx-mxqf-f9vc

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

Nextcloud

Contacts

All

All

All

All

cpe:2.3:a:nextcloud:contacts:*.*.*.*.*.*.*.*.:

No vendor comments have been submitted for this CVE

Social Mentions

Source

Title

Posted (UTC)

@CVEreport

CVE-2021-39221 : Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Contacts application... twitter.com/i/web/status/1...

2021-10-25 19:14:06

← Previous ID

Next ID →