

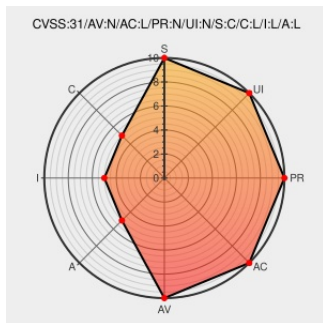


CVE-2022-31132

Published on: Not Yet Published

Last Modified on: 08/10/2022 03:35:00 PM UTC

CVE-2022-31132 - advisory for GHSA-24pm-rjfv-23mh

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

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

Nextcloud Mail is an email application for the nextcloud personal cloud product. Affected versions shipped with a CSS minifier on the path ``./vendor/cerdic/css-tidy/css_optimiser.php``. Access to the minifier is unrestricted and access may lead to Server-Side Request Forgery (SSRF). It is recommendet to upgrade to Mail 1.12.7 or Mail 1.13.6.

Users unable to upgrade may manually delete the file located at ``./vendor/cerdic/css-tidy/css_optimiser.php``

CVE-2022-31132 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version < 1.12.8

Affected Vendor/Software: **nextcloud** - **security-advisories** version >= 1.13.0, < 1.13.6

CVSS3 Score: **9.8 - CRITICAL**

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

CVE References

Description	Tags	Link
Unauthenticated SSRF in 3rd party module "cerdic/csstidy" · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	CONFIRM github.com/nextcloud/security-advisories/security/advisories/GHSA-24pm-rjfv-23mh

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,

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	Mail	All	All	All	All
cpe:2.3:a:nextcloud:mail:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-31132 : Nextcloud Mail is an email application for the nextcloud personal cloud product. Affected versions... twitter.com/i/web/status/1...	2022-08-04 17:17:24
 @Inceptus3	New Vulnerability: CVE-2022-31132 #InceptusSecure #UnderOurProtection	2022-08-04 18:13:55
 @LinInfoSec	Php - CVE-2022-31132: github.com/nextcloud/secu...	2022-08-04 19:05:54
 @threatmeter	CVE-2022-31132 Nextcloud Mail is an email application for the nextcloud personal cloud product. Affected versions s... twitter.com/i/web/status/1...	2022-08-05 07:09:34
 @phpadvisories	CVE-2022-31132 Nextcloud Mail up to 1.12.6/1.13.5 CSS Minifier css_optimiser.php server-side request forgery (GHS... twitter.com/i/web/status/1...	2022-08-05 07:13:43
 @Har_sia	CVE-2022-31132 har-sia.info/CVE-2022-31132... #HarsiaInfo	2022-08-06 07:01:09
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-31132 - Nextcloud Mail is an email application for the nextcloud personal clo... twitter.com/i/web/status/1...	2022-08-10 15:42:16

[← 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