

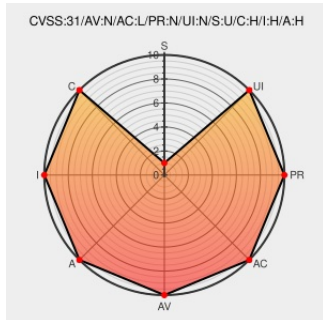


CVE-2022-21829

Published on: Not Yet Published

Last Modified on: 07/05/2022 04:55:00 PM UTC

CVE-2022-21829

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

Certain versions of [Concrete Cms](#) from [Concretecms](#) contain the following vulnerability:

Concrete CMS Versions 9.0.0 through 9.0.2 and 8.5.7 and below can download zip files over HTTP and execute code from those zip files which could lead to an RCE. Fixed by enforcing 'concrete_secure' instead of 'concrete'. Concrete now only makes requests over https even a request comes in via http. Concrete CMS security team ranked this 8 with CVSS v3.1 vector: AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H Credit goes to Anna for reporting HackerOne 1482520.

CVE-2022-21829 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **CRITICAL** severity.

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
		MISC hackerone.com/reports/1482520

hackerone.com[text/plain](#)

Inactive Link

Not Archived

h1 MISC hackerone.com/reports/1482920,8.5.8 Release Notes ::
Concrete CMSdocumentation.concretecms.org[text/html](#)MISC documentation.concretecms.org/developers/introduction/version-history/858-release-notesPage Not Found :: Concrete
CMSdocumentation.concretecms.org[text/html](#)

Inactive Link

Not Archived

MISC documentation.concretecms.org/developers/introduction/version-history/910-release-notes,

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	Concretecms	Concrete Cms	All	All	All	All
cpe:2.3:a:concretecms:concrete_cms:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-21829 : Concrete CMS Versions 9.0.0 through 9.0.2 and 8.5.7 and below can download zip files over HTTP and... twitter.com/i/web/status/1...	2022-06-24 15:18:14
 /r/netcve	CVE-2022-21829	2022-06-24 16:38:14

[← 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