

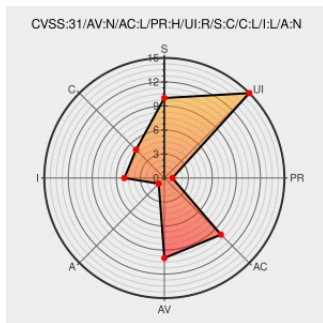


CVE-2022-43688

Published on: Not Yet Published

Last Modified on: 11/17/2022 04:58:00 AM UTC

CVE-2022-43688

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

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

Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Stored Cross-Site Scripting (XSS) in icons since the Microsoft application tile color is not sanitized. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+.

CVE-2022-43688 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Release 9.1.3 · concretecms/concretecms · GitHub	github.com text/html	MISC github.com/concretecms/concretecms/releases/9.1.3
Release 8.5.10 · concretecms/concretecms · GitHub	github.com text/html	MISC github.com/concretecms/concretecms/releases/8.5.10
Concrete CMS Security Advisory 2022-10-31	www.concretecms.org text/html	MISC www.concretecms.org/about/project-news/security/concrete-cms-security-advisory-2022-10-31
9.1.3 Release Notes :: Concrete CMS	documentation.concretecms.org text/html	MISC documentation.concretecms.org/developers/introduction/version-history/913-release-notes
8.5.10-12 Release Notes :: Concrete CMS	documentation.concretecms.org text/html	MISC documentation.concretecms.org/developers/introduction/version-history/8510-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

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Concretecms	Concrete Cms	All	All	All	All
Application	Concretecms	Concrete Cms	All	All	All	All

```
cpe:2.3:a:concretecms:concrete_cms:*:*:*:*:*:*:
```

```
cpe:2.3:a:concretecms:concrete_cms:*:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-43688 : Concrete CMS formerly concrete5 below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Stored... twitter.com/i/web/status/1...	2022-11-14 23:07:48
 /r/netcve	CVE-2022-43688	2022-11-15 00:38:39

[← 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