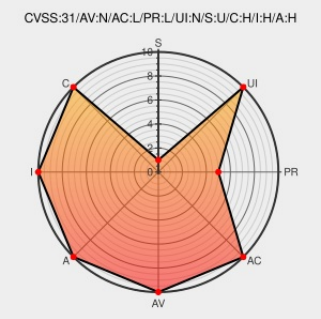
CVE-2020-35597

Published on: Not Yet Published

Last Modified on: 06/27/2022 06:24:00 PM UTC

CVE-2020-35597

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Victor Cms from Victor Cms Project contain the following vulnerability:

Victor CMS 1.0 is vulnerable to SQL injection via c_id parameter of admin_edit_comment.php, p_id parameter of admin_edit_post.php, u_id parameter of admin_edit_user.php, and edit parameter of admin_update_categories.php.

CVE-2020-35597 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Victor CMS 1.0 - Multiple SQL Injection (Authenticated) - PHP webapps Exploit	www.exploit-db.com Proof of Concept text/html	MISC www.exploit-db.com/exploits/49282
SQL Injection vulnerabilities in different features · Issue #16 ·	github.com	MISC

VictorAlagwu/CMSsite · GitHub	text/html	github.com/VictorAlagwu/CMSsite/issues/16
Victor CMS 1.0 Multiple SQL Injection (Authenticated) - CXSecurity.com	cxsecurity.com text/html	MISC cxsecurity.com/issue/WLB-2020120118

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	Victor Cms Project	Victor Cms	1.0	All	All	All

cpe:2.3:a:victor_cms_project:victor_cms:1.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-35597 : Victor CMS 1.0 is vulnerable to SQL injection via c_id parameter of admin_edit_comment.php, p_id p… twitter.com/i/web/status/1…	2022-06-16 19:06:31
@wvdsteen	New vulnerability on the NVD: CVE-2020-35597 ift.tt/fkgFGKu June 17, 2022 at 07:15AM	2022-06-16 20:16:01
@WesUncensored	New vulnerability on the NVD: CVE-2020-35597 ift.tt/fkgFGKu	2022-06-16 20:33:10
@workentin	New vulnerability on the NVD: CVE-2020-35597 ift.tt/fkgFGKu	2022-06-16 20:40:50
@xanadulinux	CVE-2020-35597 ift.tt/fkgFGKu	2022-06-16 20:52:12
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2020-35597 Victor CMS 1.0 is vulnerable to SQL injection via c_id parameter… twitter.com/i/web/status/1…	2022-06-16 20:55:59
@LinInfoSec	Php - CVE-2020-35597: cxsecurity.com/issue/WLB-2020…	2022-06-16 21:01:28
/r/netcve	CVE-2020-35597	2022-06-16 20:38:25

← 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 registred 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