

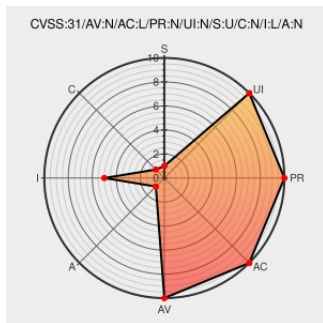


CVE-2019-8292

Published on: 10/01/2019 12:00:00 AM UTC

Last Modified on: 10/14/2022 02:49:00 AM UTC

CVE-2019-8292

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

Certain versions of [Online Store System](#) from [Online Store System Project](#) contain the following vulnerability:

Online Store System v1.0 delete_product.php doesn't check to see if a user authenticated or has administrative rights allowing arbitrary product deletion.

CVE-2019-8292 has been assigned by larry0@me.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **abcprintf** - **Online Store** version <= 1.0

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Larry Cashdollar Vulnerability	Exploit Third Party Advisory www.vapidlabs.com	MISC www.vapidlabs.com/advisory.php?v=210

	www.openwall.com text/html	
Download - Code!! , ■■■■■■■■■■ ■■■■	Product www.abcprintf.com text/html	 MISC www.abcprintf.com/view_download.php?id=17
oss-security - Re: Arbitrary file upload vulnerability in upload-image-with-ajax v1.0	www.openwall.com text/html	 MLIST [oss-security] 20191223 Re: Arbitrary file upload vulnerability in upload-image-with-ajax v1.0
oss-security - Multiple vulnerabilities in Online store system v1.0 Stored XSS and unauthenticated product deletions.	Exploit Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20191002 Multiple vulnerabilities in Online store system v1.0 Stored XSS and unauthenticated product deletions.
oss-security - Arbitrary file upload vulnerability in upload-image-with-ajax v1.0	www.openwall.com text/html	 MLIST [oss-security] 20191223 Arbitrary file upload vulnerability in upload-image-with-ajax v1.0

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	Online Store System Project	Online Store System	1.0	All	All	All
Application	Online Store System Project	Online Store System	1.0	All	All	All
cpe:2.3:a:online_store_system_project:online_store_system:1.0:****:****:						
cpe:2.3:a:online_store_system_project:online_store_system:1.0:****:****:						

No vendor comments have been submitted for this CVE

[← 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