



CVE-2020-15243

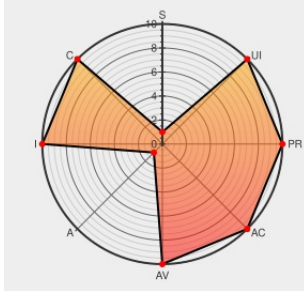
Published on: 10/08/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 04:56:00 PM UTC

CVE-2020-15243 - advisory for GHSA-8g9m-jx26-qp4h

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N



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

Affected versions of Smartstore have a missing WebApi Authentication attribute. This vulnerability affects Smartstore shops in version 4.0.0 & 4.0.1 which have installed and activated the Web API plugin. Users of Smartstore 4.0.0 and 4.0.1 must merge their repository with 4.0.x or overwrite the file SmartStore.Web.Framework in the */bin* directory of

the deployed shop with this file. As a workaround without updating uninstall the Web API plugin to close this vulnerability.

CVE-2020-15243 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: smartstore - SmartStoreNET version $\geq 4.0.0$, $\leq 4.0.1$

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

WebApi Authentication Attribute was missing. · Advisory · smartstore/SmartStoreNET · GitHub

Tags

Third Party Advisory

github.com

text/html

Link

CONFIRM

github.com/smartstore/SmartStoreNET/security/advisories/GHSA-8g9m-jx26-qp4h

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	Smartstore	Smartstore	4.0.0	All	All	All
Application	Smartstore	Smartstore	4.0.1	All	All	All
Application	Smartstore	Smartstore	4.0.0	All	All	All
Application	Smartstore	Smartstore	4.0.1	All	All	All

cpe:2.3:a:smartstore:smartstore:4.0.0:****:****:

cpe:2.3:a:smartstore:smartstore:4.0.1:****:****:

cpe:2.3:a:smartstore:smartstore:4.0.0:****:****:

cpe:2.3:a:smartstore:smartstore:4.0.1:****:****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→