



CVE-2020-15253

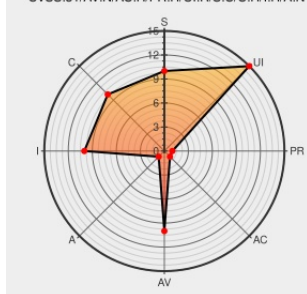
Published on: 10/14/2020 12:00:00 AM UTC

Last Modified on: 10/18/2022 08:20:00 PM UTC

CVE-2020-15253 - advisory for GHSA-7f37-2fjr-v9p7

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

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



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

Versions of Grocy <= 2.7.1 are vulnerable to Cross-Site Scripting via the Create Shopping List module, that is rendered upon deleting that Shopping List. The issue was also found in users, batteries, chores, equipment, locations, quantity units, shopping locations, tasks, taskcategories, product groups, recipes and products. Authentication is required to exploit these issues and Grocy should not be publicly exposed. The linked reference details a proof-of-concept.

CVE-2020-15253 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [grocy](#) - **grocy** version <= 2.7.1

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
XSS and HTML injection possible at some places · Advisory · grocy/grocy · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/grocy/grocy/security/advisories/GHSA-7f37-2fjr-v9p7
grocy 2.7.1 - Persistent Cross-Site Scripting - PHP webapps Exploit	www.exploit-db.com Proof of Concept text/html	 MISC www.exploit-db.com/exploits/48792
XSS and HTML Injection on Create Shopping List & shopping list item notes (Rendered upon deleting it) · Issue #996 · grocy/grocy · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	 MISC github.com/grocy/grocy/issues/996
Escape HTML (where needed, for bootbox) (references #996) · grocy/grocy@0df2590 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/grocy/grocy/commit/0df2590de27c60c18b7db6e056347bd2aff5a887
Escape shopping list item notes (references #996) · grocy/grocy@0624b0d · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/grocy/grocy/commit/0624b0df594a4353ef25e6b1874565ea52ce7772
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	Grocy	Grocy	All	All	All	All
cpe:2.3:a:grocy:grocy:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous IDNext ID →		

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)