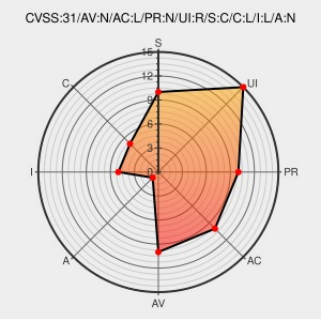
CVE-2018-25050

Published on: Not Yet Published

Last Modified on: 01/06/2023 04:53:00 PM UTC

CVE-2018-25050

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



Certain versions of Chosen from Getharvest contain the following vulnerability:

A vulnerability, which was classified as problematic, has been found in Harvest Chosen up to 1.8.6. Affected by this issue is the function AbstractChosen of the file coffee/lib/abstract-chosen.coffee. The manipulation of the argument group_label leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.8.7 is able to address this issue. The name of the patch is 77fd031d541e77510268d1041ed37798fdd1017e. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216956.

CVE-2018-25050 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVE References

Description	Tags	Link
Merge pull request #2997 from harvesthq/fix-group-label-xss-vulnerabi… · harvesthq/chosen@77fd031 · GitHub	github.com text/html	MISC github.com/harvesthq/chosen/commit/77fd031d541e77510268d1041ed37798fdd1
Release Version 1.8.7 · harvesthq/chosen · GitHub	github.com text/html	MISC github.com/harvesthq/chosen/releases/tag/v1.8.7
CVE-2018-25050 | Harvest Chosen abstract	vuldb.com	MISC vuldb.com/?id.216956

Chosen abstract-chosen.coffee AbstractChosen cross site scripting (ID 2997)	text/html Inactive Link Not Archived	
Escape the `group_label` when rendering it by satchmorun · Pull Request #2997 · harvesthq/chosen · GitHub	github.com text/html	MISC github.com/harvesthq/chosen/pull/2997
CVE-2018-25050 | Harvest Chosen abstract-chosen.coffee AbstractChosen cross site scripting (ID 2997)	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?ctiid.216956

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	Getharvest	Chosen	All	All	All	All

cpe:2.3:a:getharvest:chosen:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→