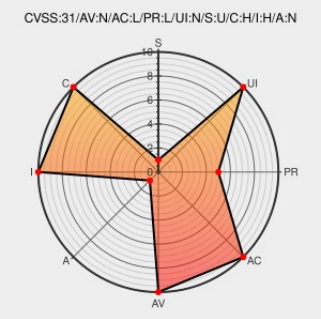
CVE-2020-15943

Published on: 08/04/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-15943

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



Certain versions of Gantt-chart from Gantt-chart Project contain the following vulnerability:

An issue was discovered in the Gantt-Chart module before 5.5.4 for Jira. Due to a missing privilege check, it is possible to read and write to the module configuration of other users. This can also be used to deliver an XSS payload to other users' dashboards. To exploit this vulnerability, an attacker has to be authenticated.

CVE-2020-15943 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
	Exploit Third Party Advisory www.syss.de	MISC www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-029.txt

	text/plain	
Gantt-Chart for Jira | Atlassian Marketplace	Product Third Party Advisory marketplace.atlassian.com text/html	MISC marketplace.atlassian.com/apps/28997/gantt-chart-for-jira?hosting=cloud&tab=overview
Full Disclosure: [SYSS-2020-029]: Jira module "Gantt-Chart for Jira" - Improper Privilege Management (CWE-269)(CVE-2020-15943)	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20200804 [SYSS-2020-029]: Jira module "Gantt-Chart for Jira" - Improper Privilege Management (CWE-269)(CVE-2020-15943)
Gantt-Chart For Jira 5.5.3 Missing Privilege Check ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158751/Gantt-Chart-For-Jira-5.5.3-Missing-Privilege-Check.html

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	Gantt-chart Project	Gantt-chart	All	All	All	All
Application	Gantt-chart Project	Gantt-chart	All	All	All	All

cpe:2.3:a:gantt-chart_project:gantt-chart:*:*:*:*:*:jira:*:*:

cpe:2.3:a:gantt-chart_project:gantt-chart:*:*:*:*:*:jira:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→