CVE-2023-5211

Published on: Not Yet Published

Last Modified on: 10/31/2023 02:23:00 PM UTC

CVE-2023-5211

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

Certain versions of Fattura24 from Unknown contain the following vulnerability:

The Fattura24 WordPress plugin before 6.2.8 does not sanitize or escape the 'id' parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting vulnerability.

CVE-2023-5211 has been assigned by contact@wpscan.com to track the vulnerability

Affected Vendor/Software: **Unknown** - **Fattura24** version **< 6.2.8**

CVE References

Description	Tags	Link
Fattura24 < 6.2.8 - Reflected Cross-Site Scripting WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/aa868380-cda7-4ec6-8a3f-d9fa692908f2

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 Software

Vendor	Product	Version
Unknown	Fattura24	< 6.2.8

No vendor comments have been submitted for this CVE

← Previous ID | Next ID→

CVE.report and Source URL Uptime Status status.cve.report