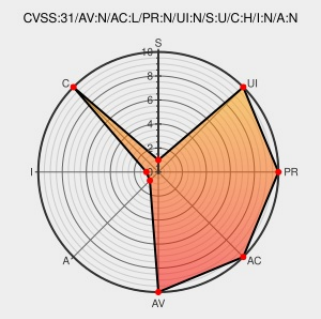
CVE-2020-25750

Published on: 09/17/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:31 PM UTC

CVE-2020-25750

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



Certain versions of Dotplant2 from Dotplant contain the following vulnerability:

** UNSUPPORTED WHEN ASSIGNED ** An issue was discovered in DotPlant2 before 2020-09-14. In class Pay2PayPayment in payment/Pay2PayPayment.php, there is an XXE vulnerability in the checkResult function. The user input ($_POST['xml']) is used for simplexml_load_string without sanitization. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2020-25750 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
XXE Vulnerability · Issue #400 · DevGroup-ru/dotplant2 · GitHub	Exploit Patch	MISC github.com/DevGroup-ru/dotplant2/issues/400

Third Party Advisory
github.com
text/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	Dotplant	Dotplant2	All	All	All	All
Application	Dotplant	Dotplant2	All	All	All	All

cpe:2.3:a:dotplant:dotplant2:*:*:*:*:*:*:*:*:

cpe:2.3:a:dotplant:dotplant2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→