



CVE-2019-12331

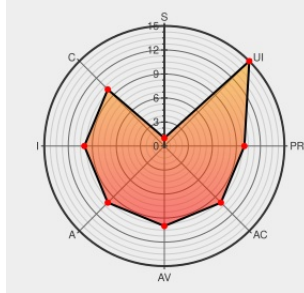
Published on: 11/07/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12331

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

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



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

PHPOffice PhpSpreadsheet before 1.8.0 has an XXE issue. The XmlScanner decodes the sheet1.xml from an .xlsx to utf-8 if something else than UTF-8 is declared in the header. This was a security measurement to prevent CVE-2018-19277 but the fix is not sufficient.

By double-encoding the the xml payload to utf-7 it is possible to bypass the check for the string '<!ENTITY' and thus allowing for an xml external entity processing (XXE) attack.

CVE-2019-12331 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Phpspreadsheet/CHANGELOG.md at	CVE-2019-12331	CONFIRM

Phpspreadsheet/CHANGELOG.md at master · PHPOffice/PhpSpreadsheet · GitHub

Third Party Advisory

github.com

text/html

CONFIRM

github.com/PHPOffice/PhpSpreadsheet/blob/master/CHANGELOG.md#180--2019-07-01

usd-2019-0046 | usd Herolab

Exploit

Third Party Advisory

herolab.usd.de

text/html

MISC

herolab.usd.de/security-advisories/usd-2019-0046/

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	Phpspreadsheet Project	Phpspreadsheet	All	All	All	All
Application	Phpspreadsheet Project	Phpspreadsheet	All	All	All	All
cpe:2.3:a:phpspreadsheet_project:phpspreadsheet:*:*:*:*:*:*:						
cpe:2.3:a:phpspreadsheet_project:phpspreadsheet:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE