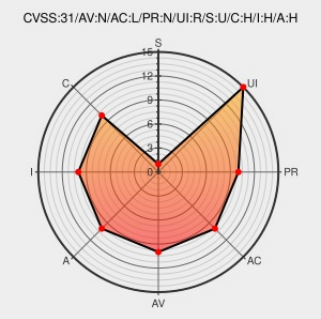
CVE-2019-12331

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



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 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	Third Party Advisory	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/

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

← Previous ID

Next ID→