



CVE-2019-12799

Published on: 06/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:40 PM UTC

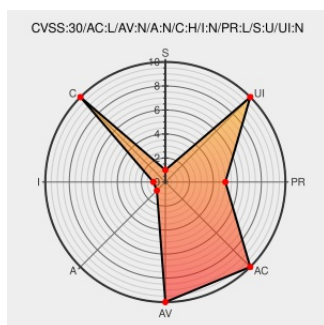
CVE-2019-12799

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

In `createInstanceFromNamedArguments` in Shopware through 5.6.x, a crafted web request can trigger a PHP object instantiation vulnerability, which can result in an arbitrary deserialization if the right class is instantiated. An attacker can leverage this deserialization to achieve remote code execution. NOTE: this issue is a bypass for a CVE-2017-18357 whitelist patch.

CVE-2019-12799 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	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Added CVE-2017 18357 - Shopware <code>createInstanceFromNamedArguments</code> PHP Object Instantiation by stevenseeley · Pull Request #11828 · rapid7/metasploit-	Issue Tracking Patch	MISC github.com/rapid7/metasploit-

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	Shopware	Shopware	All	All	All	All
cpe:2.3:a:shopware:shopware:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →