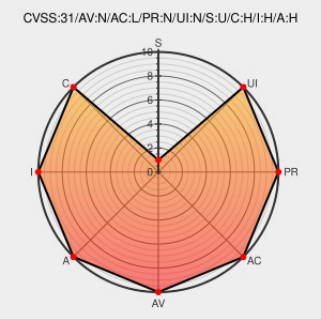
CVE-2018-6345

Published on: 01/15/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6345

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



Certain versions of Hhvm from Facebook contain the following vulnerability:

The function number_format is vulnerable to a heap overflow issue when its second argument ($dec_points) is excessively large. The internal implementation of the function will cause a string to be created with an invalid length, which can then interact poorly with other functions. This affects all supported versions of HHVM (3.30.1 and 3.27.5 and below).

CVE-2018-6345 has been assigned by cve-assign@fb.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Facebook** - **HHVM** version **!=> 3.30.2**

Affected Vendor/Software: **Facebook** - **HHVM** version **>= 3.30.0**

Affected Vendor/Software: **Facebook** - **HHVM** version **!=> 3.27.6**

Affected Vendor/Software: **Facebook** - **HHVM** version **< 3.27.6**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
HHVM 3.30.2 and 3.27.6 | HHVM	Release Notes Vendor Advisory hhvm.com text/html	MISC hhvm.com/blog/2019/01/14/hhvm-3.30.2.html
Fix a bug in number_format() · facebook/hhvm@190ffdf · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/facebook/hhvm/commit/190ffdf6c8b1ec443be202c7d69e63a7e3da25e3

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	Facebook	Hhvm	All	All	All	All
Application	Facebook	Hhvm	All	All	All	All

cpe:2.3:a:facebook:hhvm:*:*:*:*:*:*:*:*:

cpe:2.3:a:facebook:hhvm:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→