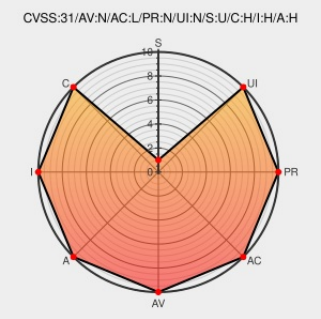
CVE-2019-19576

Published on: 12/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19576

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



Certain versions of K2 from Getk2 contain the following vulnerability:

class.upload.php in verot.net class.upload before 1.0.3 and 2.x before 2.0.4, as used in the K2 extension for Joomla! and other products, omits .phar from the set of dangerous file extensions.

CVE-2019-19576 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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
CVE-2019–19576 (Arbitrary file upload in class.upload.php) | by Jinny Ramsmark | Medium	Exploit Third Party Advisory medium.com text/html	MISC medium.com/@jra8908/cve-2019-19576-e9da712b779

GitHub - jra89/CVE-2019-19576: This is a filter bypass exploit that results in arbitrary file upload and remote code execution in class.upload.php <= 2.0.3	Exploit Third Party Advisory github.com text/html	MISC github.com/jra89/CVE-2019-19576
Web development, design and free software code - verot.net	Product www.verot.net text/html	MISC www.verot.net
blacklist .phar extension · verot/class.upload.php@5a7505d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/verot/class.upload.php/commit/5a7505ddec956fdc9e9c071ae50898
Verot 2.0.3 Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155577/Verot-2.0.3-Remote-Code-Exec
verot.net - class.upload.php	Vendor Advisory www.verot.net text/html	MISC www.verot.net/php_class_upload.htm
Comparing 2.0.3...2.0.4 · verot/class.upload.php · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/verot/class.upload.php/compare/2.0.3...2.0.4
Comparing 1.0.2...1.0.3 · verot/class.upload.php · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/verot/class.upload.php/compare/1.0.2...1.0.3
blacklist .phar extension · verot/class.upload.php@db1b4fe · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/verot/class.upload.php/commit/db1b4fe50c1754696970d8b437f07e
Update class.upload.php · getk2/k2@d134470 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/getk2/k2/commit/d1344706c4b74c2ae7659b286b5a06611

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This is a filter bypass exploit that results in arbitrary file upload and remote code execution in class.upload.php <…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Getk2	K2	All	All	All	All
Application	Getk2	K2	All	All	All	All
Application	Verot Project	Verot	All	All	All	All
Application	Verot Project	Verot	All	All	All	All

cpe:2.3:a:getk2:k2:*:*:*:*:*:joomla!:*:*:

cpe:2.3:a:getk2:k2:*:*:*:*:*:joomla\!:*:*:

cpe:2.3:a:verot_project:verot:*:*:*:*:*:*:*:*:

cpe:2.3:a:verot_project:verot:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→