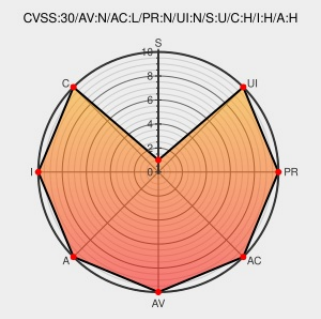
CVE-2018-16283

Published on: 09/24/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:34 PM UTC

CVE-2018-16283

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



Certain versions of Wechat Brodcast from Wechat Brodcast Project contain the following vulnerability:

The Wechat Broadcast plugin 1.2.0 and earlier for WordPress allows Directory Traversal via the Image.php url parameter.

CVE-2018-16283 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
Vulnerability Local File Inclusion · Issue #14 · springjk/wordpress-wechat-broadcast · GitHub	Issue Tracking Third Party Advisory github.com text/html	CONFIRM github.com/springjk/wordpress-wechat-broadcast/issues/14

Full Disclosure: WordPress Plugin Wechat Broadcast 1.2.0 - Local/Remote File Inclusion	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20180920 WordPress Plugin Wechat Broadcast 1.2.0 - Local/Remote File Inclusion
Wechat Broadcast <= 1.2.0 - Local/Remote File Inclusion	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC wpvulndb.com/vulnerabilities/9132
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	MISC exchange.xforce.ibmcloud.com/vulnerabilities/150202
WordPress Plugin Wechat Broadcast 1.2.0 - Local File Inclusion - PHP webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 45438

There are currently no QIDs associated with this CVE

Exploit/POC from Github

cve-2018-16283

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wechat Brodcast Project	Wechat Brodcast	All	All	All	All

cpe:2.3:a:wechat_brodcast_project:wechat_brodcast:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report