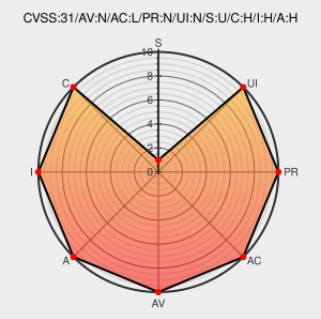
CVE-2017-17671

Published on: 12/13/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:26 PM UTC

CVE-2017-17671

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



Certain versions of Windows from Microsoft contain the following vulnerability:

vBulletin through 5.3.x on Windows allows remote PHP code execution because a require_once call is reachable with an unauthenticated request that can include directory traversal sequences to specify an arbitrary pathname, and because ../ traversal is blocked but ..\ traversal is not blocked. For example, an attacker can make an invalid HTTP request containing PHP code, and then make an index.php?routestring= request with enough instances of ".." to reach an Apache HTTP Server log file.

CVE-2017-17671 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
401 Authorization Required	Exploit	MISC blogs.securiteam.com/index.php/archives/3569

401 Authorization Required

Exploit
Third Party Advisory
blogs.securiteam.com
text/html
Inactive Link Not Archived

MISC blogs.securiteam.com/index.php/archives/3569

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
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Vbulletin	Vbulletin	5.0.0	beta_11	All	All
Application	Vbulletin	Vbulletin	5.0.0	beta_28	All	All
Application	Vbulletin	Vbulletin	5.0.0	beta_11	All	All
Application	Vbulletin	Vbulletin	5.0.0	beta_28	All	All
Application	Vbulletin	Vbulletin	All	All	All	All

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.0:beta_11:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.0:beta_28:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.0:beta_11:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.0:beta_28:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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