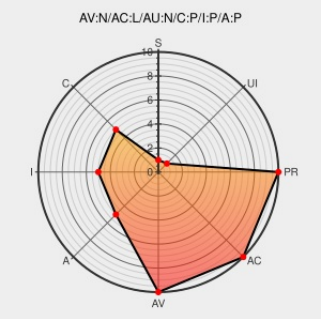
CVE-2015-7808

Published on: 11/24/2015 12:00:00 AM UTC

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

CVE-2015-7808

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



Certain versions of Vbulletin from Vbulletin contain the following vulnerability:

The vB_Api_Hook::decodeArguments method in vBulletin 5 Connect 5.1.2 through 5.1.9 allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via a crafted serialized object in the arguments parameter to ajax/api/hook/decodeArguments.

CVE-2015-7808 has been assigned by cve@mitre.org to track the vulnerability

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
vBulletin 5.1.x - Remote Code Execution - PHP webapps Exploit	Exploit, www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 38629
vBulletin Exploits in the Wild - Sucuri Blog	Exploit, blog.sucuri.net, text/html	MISC blog.sucuri.net/2015/11/vbulletin-exploits-in-the-wild.html
Private Paste - Pastie	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	MISC pastie.org/pastes/10527766/text?key=wq1hgkcj4afb9ipqzllsq
vBulletin 5.1.2 Unserialize Code Execution	Exploit	MISC packetstormsecurity.com/files/134331/vBulletin-5.1.2-

≈ Packet Storm	packetstormsecurity.com text/html	Unserialize-Code-Execution.html
CVE-2015-7808 vBulletin 5.1.2 Unserialize Code Execution | Rapid7	Exploit www.rapid7.com text/html	MISC www.rapid7.com/db/modules/exploit/multi/http/vbulletin_unserialize
Check Point Discovers Critical vBulletin 0-Day	Exploit blog.checkpoint.com text/html	MISC blog.checkpoint.com/2015/11/05/check-point-discovers-critical-vbulletin-0-day/

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC code for vBulletin PreAuth vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vbulletin	Vbulletin	5.0.0	All	All	All
Application	Vbulletin	Vbulletin	5.0.1	All	All	All
Application	Vbulletin	Vbulletin	5.0.2	All	All	All
Application	Vbulletin	Vbulletin	5.0.3	All	All	All
Application	Vbulletin	Vbulletin	5.0.4	All	All	All
Application	Vbulletin	Vbulletin	5.0.5	All	All	All
Application	Vbulletin	Vbulletin	5.1.0	All	All	All
Application	Vbulletin	Vbulletin	5.1.0	rc1	All	All
Application	Vbulletin	Vbulletin	5.1.1	All	All	All
Application	Vbulletin	Vbulletin	5.1.2	All	All	All
Application	Vbulletin	Vbulletin	5.1.2	beta1	All	All
Application	Vbulletin	Vbulletin	5.1.2	rc1	All	All
Application	Vbulletin	Vbulletin	5.1.2	rc2	All	All
Application	Vbulletin	Vbulletin	5.1.3	All	All	All
Application	Vbulletin	Vbulletin	5.1.3	alpha5	All	All
Application	Vbulletin	Vbulletin	5.1.4	All	All	All
Application	Vbulletin	Vbulletin	5.1.5	All	All	All
Application	Vbulletin	Vbulletin	5.1.6	All	All	All
Application	Vbulletin	Vbulletin	5.1.7	All	All	All

Application	Vbulletin	Vbulletin	5.1.8	All	All	All
Application	Vbulletin	Vbulletin	5.1.9	All	All	All
Application	Vbulletin	Vbulletin	5.0.0	All	All	All
Application	Vbulletin	Vbulletin	5.0.1	All	All	All
Application	Vbulletin	Vbulletin	5.0.2	All	All	All
Application	Vbulletin	Vbulletin	5.0.3	All	All	All
Application	Vbulletin	Vbulletin	5.0.4	All	All	All
Application	Vbulletin	Vbulletin	5.0.5	All	All	All
Application	Vbulletin	Vbulletin	5.1.0	All	All	All
Application	Vbulletin	Vbulletin	5.1.0	rc1	All	All
Application	Vbulletin	Vbulletin	5.1.1	All	All	All
Application	Vbulletin	Vbulletin	5.1.2	All	All	All
Application	Vbulletin	Vbulletin	5.1.2	beta1	All	All
Application	Vbulletin	Vbulletin	5.1.2	rc1	All	All
Application	Vbulletin	Vbulletin	5.1.2	rc2	All	All
Application	Vbulletin	Vbulletin	5.1.3	All	All	All
Application	Vbulletin	Vbulletin	5.1.3	alpha5	All	All
Application	Vbulletin	Vbulletin	5.1.4	All	All	All
Application	Vbulletin	Vbulletin	5.1.5	All	All	All
Application	Vbulletin	Vbulletin	5.1.6	All	All	All
Application	Vbulletin	Vbulletin	5.1.7	All	All	All
Application	Vbulletin	Vbulletin	5.1.8	All	All	All
Application	Vbulletin	Vbulletin	5.1.9	All	All	All

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

cpe:2.3:a:vbulletin:vbulletin:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.2:beta1:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.2:rc2:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.3:alpha5:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.7:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.9:*:*:*:*:*:*:*:

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

cpe:2.3:a:vbulletin:vbulletin:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.2:beta1:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.2:rc2:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.3:alpha5:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:vbulletin:vbulletin:5.1.6:*:*:*:*:*:*:*

cpe:2.3:a:vbulletin:vbulletin:5.1.7:*:*:*:*:*:*:*

cpe:2.3:a:vbulletin:vbulletin:5.1.8:*:*:*:*:*:*:*

cpe:2.3:a:vbulletin:vbulletin:5.1.9:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→