



CVE-2011-5251

Published on: 12/31/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:17 PM UTC

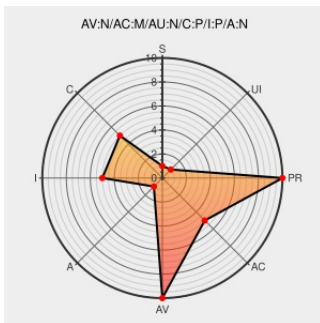
CVE-2011-5251

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Vbulletin](#) from [Vbulletin](#) contain the following vulnerability:

Open redirect vulnerability in forum/login.php in vBulletin 4.1.3 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the url parameter in a lostpw action.

CVE-2011-5251 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Potential Phishing Vector - vBulletin Community Forum

[www.vbulletin.com
text/html](http://www.vbulletin.com/text/html)

[CONFIRM www.vbulletin.com/forum/showthread.php/381014-Potential-Phishing-Vector?p=2166441](http://www.vbulletin.com/forum/showthread.php/381014-Potential-Phishing-Vector?p=2166441)

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	Vbulletin	Vbulletin	4.0.0	All	All	All
Application	Vbulletin	Vbulletin	4.0.1	All	All	All
Application	Vbulletin	Vbulletin	4.0.2	All	All	All
Application	Vbulletin	Vbulletin	4.0.3	All	All	All
Application	Vbulletin	Vbulletin	4.0.4	All	All	All
Application	Vbulletin	Vbulletin	4.0.5	All	All	All
Application	Vbulletin	Vbulletin	4.0.6	All	All	All
Application	Vbulletin	Vbulletin	4.0.7	All	All	All
Application	Vbulletin	Vbulletin	4.0.8	All	All	All
Application	Vbulletin	Vbulletin	4.1	All	All	All
Application	Vbulletin	Vbulletin	4.1.1	All	All	All
Application	Vbulletin	Vbulletin	4.1.2	All	All	All
Application	Vbulletin	Vbulletin	4.0.0	All	All	All
Application	Vbulletin	Vbulletin	4.0.1	All	All	All
Application	Vbulletin	Vbulletin	4.0.2	All	All	All
Application	Vbulletin	Vbulletin	4.0.3	All	All	All
Application	Vbulletin	Vbulletin	4.0.4	All	All	All
Application	Vbulletin	Vbulletin	4.0.5	All	All	All
Application	Vbulletin	Vbulletin	4.0.6	All	All	All
Application	Vbulletin	Vbulletin	4.0.7	All	All	All
Application	Vbulletin	Vbulletin	4.0.8	All	All	All
Application	Vbulletin	Vbulletin	4.1	All	All	All
Application	Vbulletin	Vbulletin	4.1.1	All	All	All
Application	Vbulletin	Vbulletin	4.1.2	All	All	All
Application	Vbulletin	Vbulletin	All	All	All	All
cpe:2.3:a:vbulletin:vbulletin:4.0.0:****:***:						
cpe:2.3:a:vbulletin:vbulletin:4.0.1:****:***:						
cpe:2.3:a:vbulletin:vbulletin:4.0.2:****:***:						
cpe:2.3:a:vbulletin:vbulletin:4.0.3:****:***:						
cpe:2.3:a:vbulletin:vbulletin:4.0.4:****:***:						
cpe:2.3:a:vbulletin:vbulletin:4.0.5:****:***:						
cpe:2.3:a:vbulletin:vbulletin:4.0.6:****:***:						
cpe:2.3:a:vbulletin:vbulletin:4.0.7:****:***:						

cpe:2.3:a:vbulletin:vbulletin:4.0.8:*****:
cpe:2.3:a:vbulletin:vbulletin:4.1:*****:
cpe:2.3:a:vbulletin:vbulletin:4.1.1:*****:
cpe:2.3:a:vbulletin:vbulletin:4.1.2:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.0:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.1:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.2:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.3:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.4:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.5:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.6:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.7:*****:
cpe:2.3:a:vbulletin:vbulletin:4.0.8:*****:
cpe:2.3:a:vbulletin:vbulletin:4.1:*****:
cpe:2.3:a:vbulletin:vbulletin:4.1.1:*****:
cpe:2.3:a:vbulletin:vbulletin:4.1.2:*****:
cpe:2.3:a:vbulletin:vbulletin:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)