



CVE-2004-1822

Published on: 03/15/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1822

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Multiple cross-site scripting (XSS) vulnerabilities in Phorum 3.1 through 5.0.3 beta allow remote attackers to inject arbitrary web script or HTML via the (1) HTTP_REFERER parameter to login.php, (2) HTTP_REFERER parameter to register.php, or (3) target parameter to profile.php.

CVE-2004-1822 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

SecurityTracker.com Archives - Phorum HTTP_REFERER and Other Input Validation Flaw Permits Cross-Site Scripting Attacks

[securitytracker.com](#)
[text/html](#)

[SECTrack 1009433](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 4334](#)

Inactive Link Not Archived

404 Not Found

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[CONFIRM](#)
[phorum.org/changelog.txt](#)

Inactive Link Not Archived

Secunia - Advisories - Phorum "HTTP_REFERER" Cross Site Scripting Vulnerabilities

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)

[SECUNIA 11157](#)

text/html

No Description Provided

www.osvdb.org

OSVDB 4335

Inactive Link Not Archived

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

XF phorum-register-xss(15494)

'Phorum 5.0.3 Beta && Earlier XSS Issues' - MARC

marc.info
text/html

BUGTRAQ 20040315
Phorum 5.0.3 Beta &&
Earlier XSS Issues

Phorum Multiple Module Cross-Site Scripting Vulnerability

Patch
Vendor Advisory
cve.report (archive)
text/html

BID 9882

No Description Provided

www.osvdb.org

OSVDB 4333

Inactive Link Not Archived

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	Phorum	Phorum	3.1	All	All	All
Application	Phorum	Phorum	3.1.1	All	All	All
Application	Phorum	Phorum	3.1.1a	All	All	All
Application	Phorum	Phorum	3.1.1_pre	All	All	All
Application	Phorum	Phorum	3.1.1_rc2	All	All	All
Application	Phorum	Phorum	3.1.2	All	All	All
Application	Phorum	Phorum	3.2	All	All	All
Application	Phorum	Phorum	3.2.2	All	All	All
Application	Phorum	Phorum	3.2.3	All	All	All
Application	Phorum	Phorum	3.2.3a	All	All	All
Application	Phorum	Phorum	3.2.3b	All	All	All
Application	Phorum	Phorum	3.2.4	All	All	All
Application	Phorum	Phorum	3.2.5	All	All	All
Application	Phorum	Phorum	3.2.6	All	All	All
Application	Phorum	Phorum	3.2.7	All	All	All
Application	Phorum	Phorum	3.2.8	All	All	All
Application	Phorum	Phorum	3.2.9	All	All	All

Application	Phorum	Phorum	3.3.1	All	All	All
Application	Phorum	Phorum	3.3.1a	All	All	All
Application	Phorum	Phorum	3.3.2	All	All	All
Application	Phorum	Phorum	3.3.2a	All	All	All
Application	Phorum	Phorum	3.3.2b3	All	All	All
Application	Phorum	Phorum	3.4	All	All	All
Application	Phorum	Phorum	3.4.1	All	All	All
Application	Phorum	Phorum	3.4.2	All	All	All
Application	Phorum	Phorum	3.4.3	All	All	All
Application	Phorum	Phorum	3.4.4	All	All	All
Application	Phorum	Phorum	3.4.5	All	All	All
Application	Phorum	Phorum	3.4.6	All	All	All
Application	Phorum	Phorum	5.0.3_beta	All	All	All
Application	Phorum	Phorum	3.1	All	All	All
Application	Phorum	Phorum	3.1.1	All	All	All
Application	Phorum	Phorum	3.1.1a	All	All	All
Application	Phorum	Phorum	3.1.1_pre	All	All	All
Application	Phorum	Phorum	3.1.1_rc2	All	All	All
Application	Phorum	Phorum	3.1.2	All	All	All
Application	Phorum	Phorum	3.2	All	All	All
Application	Phorum	Phorum	3.2.2	All	All	All
Application	Phorum	Phorum	3.2.3	All	All	All
Application	Phorum	Phorum	3.2.3a	All	All	All
Application	Phorum	Phorum	3.2.3b	All	All	All
Application	Phorum	Phorum	3.2.4	All	All	All
Application	Phorum	Phorum	3.2.5	All	All	All
Application	Phorum	Phorum	3.2.6	All	All	All
Application	Phorum	Phorum	3.2.7	All	All	All
Application	Phorum	Phorum	3.2.8	All	All	All
Application	Phorum	Phorum	3.3.1	All	All	All
Application	Phorum	Phorum	3.3.1a	All	All	All
Application	Phorum	Phorum	3.3.2	All	All	All
Application	Phorum	Phorum	3.3.2a	All	All	All
Application	Phorum	Phorum	3.3.2b3	All	All	All
Application	Phorum	Phorum	3.4	All	All	All
Application	Phorum	Phorum	3.4.1	All	All	All

Application	Phorum	Phorum	3.4.2	All	All	All
Application	Phorum	Phorum	3.4.3	All	All	All
Application	Phorum	Phorum	3.4.4	All	All	All
Application	Phorum	Phorum	3.4.5	All	All	All
Application	Phorum	Phorum	3.4.6	All	All	All
Application	Phorum	Phorum	5.0.3_beta	All	All	All
cpe:2.3:a:phorum:phorum:3.1:*****:						
cpe:2.3:a:phorum:phorum:3.1.1:*****:						
cpe:2.3:a:phorum:phorum:3.1.1a:*****:						
cpe:2.3:a:phorum:phorum:3.1.1_pre:*****:						
cpe:2.3:a:phorum:phorum:3.1.1_rc2:*****:						
cpe:2.3:a:phorum:phorum:3.1.2:*****:						
cpe:2.3:a:phorum:phorum:3.2:*****:						
cpe:2.3:a:phorum:phorum:3.2.2:*****:						
cpe:2.3:a:phorum:phorum:3.2.3:*****:						
cpe:2.3:a:phorum:phorum:3.2.3a:*****:						
cpe:2.3:a:phorum:phorum:3.2.3b:*****:						
cpe:2.3:a:phorum:phorum:3.2.4:*****:						
cpe:2.3:a:phorum:phorum:3.2.5:*****:						
cpe:2.3:a:phorum:phorum:3.2.6:*****:						
cpe:2.3:a:phorum:phorum:3.2.7:*****:						
cpe:2.3:a:phorum:phorum:3.2.8:*****:						
cpe:2.3:a:phorum:phorum:3.3.1:*****:						
cpe:2.3:a:phorum:phorum:3.3.1a:*****:						
cpe:2.3:a:phorum:phorum:3.3.2:*****:						
cpe:2.3:a:phorum:phorum:3.3.2a:*****:						
cpe:2.3:a:phorum:phorum:3.3.2b3:*****:						
cpe:2.3:a:phorum:phorum:3.4:*****:						
cpe:2.3:a:phorum:phorum:3.4.1:*****:						

cpe:2.3:a:phorum:phorum:3.4.2:~::~::~:
cpe:2.3:a:phorum:phorum:3.4.3:~::~::~:
cpe:2.3:a:phorum:phorum:3.4.4:~::~::~:
cpe:2.3:a:phorum:phorum:3.4.5:~::~::~:
cpe:2.3:a:phorum:phorum:3.4.6:~::~::~:
cpe:2.3:a:phorum:phorum:5.0.3_beta:~::~::~:
cpe:2.3:a:phorum:phorum:3.1:~::~::~:
cpe:2.3:a:phorum:phorum:3.1.1:~::~::~:
cpe:2.3:a:phorum:phorum:3.1.1a:~::~::~:
cpe:2.3:a:phorum:phorum:3.1.1_pre:~::~::~:
cpe:2.3:a:phorum:phorum:3.1.1_rc2:~::~::~:
cpe:2.3:a:phorum:phorum:3.1.2:~::~::~:
cpe:2.3:a:phorum:phorum:3.2:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.2:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.3:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.3a:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.3b:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.4:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.5:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.6:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.7:~::~::~:
cpe:2.3:a:phorum:phorum:3.2.8:~::~::~:
cpe:2.3:a:phorum:phorum:3.3.1:~::~::~:
cpe:2.3:a:phorum:phorum:3.3.1a:~::~::~:
cpe:2.3:a:phorum:phorum:3.3.2:~::~::~:
cpe:2.3:a:phorum:phorum:3.3.2a:~::~::~:
cpe:2.3:a:phorum:phorum:3.3.2b3:~::~::~:
cpe:2.3:a:phorum:phorum:3.4:~::~::~:
cpe:2.3:a:phorum:phorum:3.4.1:~::~::~:

cpe:2.3:a:phorum:phorum:3.4.2:*:*:*:*:*:
cpe:2.3:a:phorum:phorum:3.4.3:*:*:*:*:*:
cpe:2.3:a:phorum:phorum:3.4.4:*:*:*:*:*:
cpe:2.3:a:phorum:phorum:3.4.5:*:*:*:*:*:
cpe:2.3:a:phorum:phorum:3.4.6:*:*:*:*:*:
cpe:2.3:a:phorum:phorum:5.0.3_beta:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)