

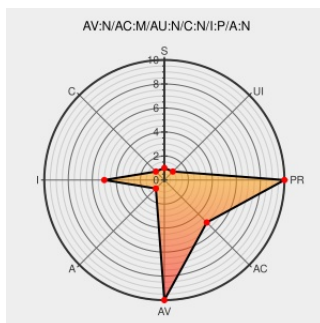


CVE-2005-2836

Published on: 09/07/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2836

[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 5.0.17a and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the username parameter to register.php or (2) a signature of a logged-in user in "My Control Center," which is not properly handled by control.php.

CVE-2005-2836 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

Secunia - Advisories - Phorum "Username" Script Insertion Vulnerability

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

[X](#) [SECUNIA 16667](#)

Neohapsis Archives - Full Disclosure List - #0048 - Re: [Full-disclosure] Multiple Phorum XSS and Session Hijacking vulnerabilities

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[F](#) [FULLDISC 20050902 Re: Multiple Phorum XSS and Session Hijacking vulnerabilities](#)

Neohapsis Archives - Full Disclosure List - #0018 - [Full-disclosure] Multiple Phorum XSS and Session Hijacking vulnerabilities

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

[F](#) [FULLDISC 20050901 Multiple Phorum XSS and Session Hijacking vulnerabilities](#)

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	3.3.1	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	3.4.7	All	All	All
Application	Phorum	Phorum	3.4.8	All	All	All
Application	Phorum	Phorum	4.3.7	All	All	All
Application	Phorum	Phorum	5.0.10	All	All	All
Application	Phorum	Phorum	5.0.11	All	All	All
Application	Phorum	Phorum	5.0.12	All	All	All
Application	Phorum	Phorum	5.0.14	All	All	All
Application	Phorum	Phorum	5.0.14a	All	All	All
Application	Phorum	Phorum	5.0.15	All	All	All
Application	Phorum	Phorum	5.0.16	All	All	All
Application	Phorum	Phorum	5.0.17	All	All	All
Application	Phorum	Phorum	5.0.3_beta	All	All	All
Application	Phorum	Phorum	5.0.7_beta	All	All	All
Application	Phorum	Phorum	5.0.9	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	3.4.7	All	All	All
Application	Phorum	Phorum	3.4.8	All	All	All
Application	Phorum	Phorum	4.3.7	All	All	All
Application	Phorum	Phorum	5.0.10	All	All	All
Application	Phorum	Phorum	5.0.11	All	All	All
Application	Phorum	Phorum	5.0.12	All	All	All
Application	Phorum	Phorum	5.0.14	All	All	All
Application	Phorum	Phorum	5.0.14a	All	All	All
Application	Phorum	Phorum	5.0.15	All	All	All
Application	Phorum	Phorum	5.0.16	All	All	All
Application	Phorum	Phorum	5.0.17	All	All	All
Application	Phorum	Phorum	5.0.3_beta	All	All	All
Application	Phorum	Phorum	5.0.7_beta	All	All	All
Application	Phorum	Phorum	5.0.9	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:3.4.7:*****:
cpe:2.3:a:phorum:phorum:3.4.8:*****:
cpe:2.3:a:phorum:phorum:4.3.7:*****:
cpe:2.3:a:phorum:phorum:5.0.10:*****:
cpe:2.3:a:phorum:phorum:5.0.11:*****:
cpe:2.3:a:phorum:phorum:5.0.12:*****:
cpe:2.3:a:phorum:phorum:5.0.14:*****:
cpe:2.3:a:phorum:phorum:5.0.14a:*****:
cpe:2.3:a:phorum:phorum:5.0.15:*****:
cpe:2.3:a:phorum:phorum:5.0.16:*****:
cpe:2.3:a:phorum:phorum:5.0.17:*****:

cpe:2.3:a:phorum:phorum:5.0.3_beta:*****:
cpe:2.3:a:phorum:phorum:5.0.7_beta:*****:
cpe:2.3:a:phorum:phorum:5.0.9:*****:
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:3.4.7:*****:
cpe:2.3:a:phorum:phorum:3.4.8:*****:
cpe:2.3:a:phorum:phorum:4.3.7:*****:
cpe:2.3:a:phorum:phorum:5.0.10:*****:
cpe:2.3:a:phorum:phorum:5.0.11:*****:
cpe:2.3:a:phorum:phorum:5.0.12:*****:
cpe:2.3:a:phorum:phorum:5.0.14:*****:
cpe:2.3:a:phorum:phorum:5.0.14a:*****:
cpe:2.3:a:phorum:phorum:5.0.15:*****:
cpe:2.3:a:phorum:phorum:5.0.16:*****:
cpe:2.3:a:phorum:phorum:5.0.17:*****:
cpe:2.3:a:phorum:phorum:5.0.3_beta:*****:
cpe:2.3:a:phorum:phorum:5.0.7_beta:*****:
cpe:2.3:a:phorum:phorum:5.0.9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)