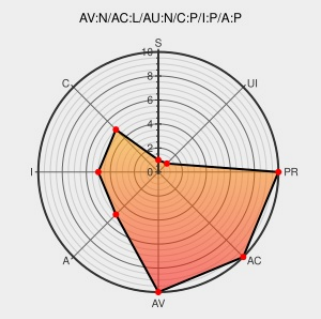
CVE-2005-4135

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

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4135

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



Certain versions of Simplebbs from Simplemedia contain the following vulnerability:

Direct static code injection vulnerability in includes/newtopic.php in SimpleBBS 1.1 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in the Host header (possibly the name parameter or variable), which is then written to data/topics.php.

CVE-2005-4135 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
SecurityTracker.com Archives - SimpleBBS Input Validation Hole in 'name' Parameter Lets Remote Users Execute Arbitrary Commands	securitytracker.com, text/html	SECTRACK 1015323
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2005-2807
SimpleBBS PHP Code Injection and Local File Inclusion Vulnerabilities - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 17949
SimpleBBS Remote Arbitrary Command Execution Vulnerability	Exploit, cve.report (archive), text/html	BID 15764
SecurityFocus	www.securityfocus.com, text/x-c	BUGTRAQ 20051207 SimpleBBS <= v1.1 remote commands execution in c by: unitedasia security crew

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	Simplemedia	Simplebbs	1.0.6	All	All	All
Application	Simplemedia	Simplebbs	1.0.7	All	All	All
Application	Simplemedia	Simplebbs	1.1	All	All	All
Application	Simplemedia	Simplebbs	1.0.6	All	All	All
Application	Simplemedia	Simplebbs	1.0.7	All	All	All
Application	Simplemedia	Simplebbs	1.1	All	All	All

cpe:2.3:a:simplemedia:simplebbs:1.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:simplemedia:simplebbs:1.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:simplemedia:simplebbs:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:simplemedia:simplebbs:1.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:simplemedia:simplebbs:1.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:simplemedia:simplebbs:1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→