



CVE-2005-1023

Published on: 04/09/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1023

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Php-nuke](#) from [Francisco Burzi](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in PHP-Nuke 6.x to 7.6 allow remote attackers to inject arbitrary web script or HTML via the (1) min parameter to the Search module, (2) the categories parameter to the FAQ module, or (3) the ltr parameter to the Encyclopedia module. NOTE: the bid parameter issue in banners.php is already an item in CVE-2005-1000.

CVE-2005-1023 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

No Description Provided

[marc.info](#)
[text/html](#)

[BUGTRAQ 20050403 Full path disclosure and XSS in PHPNuke](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF phpnuke-modulesphp-xss\(19952\)](#)

SecurityReason

[www.securityreason.com](#)
[text/html](#)

[MISC www.securityreason.com/adv/PHPNuke%206.x-7.6-p1.txt](#)

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

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	Francisco Burzi	Php-nuke	6.0	All	All	All
Application	Francisco Burzi	Php-nuke	6.5	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_beta1	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_final	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_rc1	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_rc2	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_rc3	All	All	All
Application	Francisco Burzi	Php-nuke	6.6	All	All	All
Application	Francisco Burzi	Php-nuke	6.7	All	All	All
Application	Francisco Burzi	Php-nuke	6.9	All	All	All
Application	Francisco Burzi	Php-nuke	7.0	All	All	All
Application	Francisco Burzi	Php-nuke	7.0_final	All	All	All
Application	Francisco Burzi	Php-nuke	7.1	All	All	All
Application	Francisco Burzi	Php-nuke	7.2	All	All	All
Application	Francisco Burzi	Php-nuke	7.3	All	All	All
Application	Francisco Burzi	Php-nuke	7.4	All	All	All
Application	Francisco Burzi	Php-nuke	7.5	All	All	All
Application	Francisco Burzi	Php-nuke	7.6	All	All	All
Application	Francisco Burzi	Php-nuke	6.0	All	All	All
Application	Francisco Burzi	Php-nuke	6.5	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_beta1	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_final	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_rc1	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_rc2	All	All	All
Application	Francisco Burzi	Php-nuke	6.5_rc3	All	All	All
Application	Francisco Burzi	Php-nuke	6.6	All	All	All
Application	Francisco Burzi	Php-nuke	6.7	All	All	All
Application	Francisco Burzi	Php-nuke	6.9	All	All	All
Application	Francisco Burzi	Php-nuke	7.0	All	All	All
Application	Francisco Burzi	Php-nuke	7.0_final	All	All	All

Application	Francisco Burzi	Php-nuke	7.1	All	All	All
Application	Francisco Burzi	Php-nuke	7.2	All	All	All
Application	Francisco Burzi	Php-nuke	7.3	All	All	All
Application	Francisco Burzi	Php-nuke	7.4	All	All	All
Application	Francisco Burzi	Php-nuke	7.5	All	All	All
Application	Francisco Burzi	Php-nuke	7.6	All	All	All
cpe:2.3:a:francisco_burzi:php-nuke:6.0:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_beta1:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_final:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_rc1:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_rc2:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_rc3:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.6:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.7:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.9:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:7.0:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:7.0_final:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:7.1:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:7.2:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:7.3:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:7.4:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:7.5:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:7.6:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.0:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_beta1:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_final:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_rc1:*:*:*:*:*:						
cpe:2.3:a:francisco_burzi:php-nuke:6.5_rc2:*:*:*:*:*:						

cpe:2.3:a:francisco_burzi:php-nuke:6.5_rc3:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:6.6:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:6.7:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:6.9:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:7.0:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:7.0_final:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:7.1:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:7.2:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:7.3:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:7.4:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:7.5:~::~::~::~:
cpe:2.3:a:francisco_burzi:php-nuke:7.6:~::~::~::~:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)