



CVE-2004-2020

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

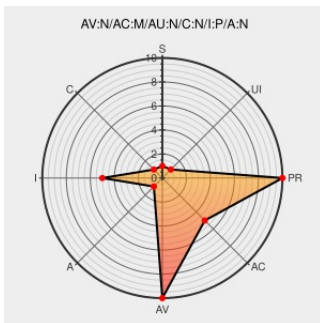
CVE-2004-2020

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 through 7.3 allow remote attackers to inject arbitrary HTML or web script into the (1) optionbox parameter in the News module, (2) date parameter in the Statistics module, (3) year, month, and month_1 parameters in the Stories_Archive module, (4) mode, order, and thold parameters in the Surveys module, or (5) a SQL statement to index.php, as processed by mainfile.php.

CVE-2004-2020 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

No Description Provided

www.osvdb.org

[OSVDB 6226](https://osvdb.org/entry/view/entry?id=6226)

Inactive Link Not Archived

No Description Provided

www.osvdb.org

[OSVDB 6225](https://osvdb.org/entry/view/entry?id=6225)

Inactive Link Not Archived

Waraxe IT Security Portal

Exploit

www.waraxe.us

text/html

[MISC www.waraxe.us/index.php?modname=sa&id=29](http://www.waraxe.us/index.php?modname=sa&id=29)

PHP-Nuke Multiple Input Validation Vulnerabilities	Exploit cve.report (archive) text/html	BID 10367
'[waraxe-2004-SA#030 - Multiple vulnerabilities in PhpNuke 6.x - 7.3]' - MARC	marc.info text/html	BUGTRAQ 20040517 [waraxe-2004-SA#030 - Multiple vulnerabilities in PhpNuke 6.x - 7.3]
Secunia - Advisories - PHP-Nuke Multiple Vulnerabilities	Exploit web.archive.org text/html	SECUNIA 11625
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phpnuke-multi-xss(16172)

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	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	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
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: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:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)