



CVE-2004-1842

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

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

CVE-2004-1842

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

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

Cross-site request forgery (CSRF) vulnerability in Php-Nuke 6.x through 7.1.0 allows remote attackers to gain administrative privileges via an img tag with a URL to admin.php.

CVE-2004-1842 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF phpnuke-img-gain-privileges\(15596\)](#)

Secunia - Advisories - PHP-Nuke Script
Insertion Vulnerabilities

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

[SECUNIA 11195](#)

PHP-Nuke Image Tag Admin Command
Execution Vulnerability

[Exploit](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 9895](#)

'[waraxe-2004-SA#008 - easy way to get
superadmin rights in' - MARC

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

[BUGTRAQ 20040322 \[waraxe-2004-SA#008 - easy way to get superadmin rights in PhpNuke 6.x-7.1.0\]](#)

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

This report does not endorse any commercial products that may be mentioned on these pages. 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	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

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: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:::~::~::
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)