



CVE-2004-1932

Published on: 04/12/2004 04:00:00 AM UTC

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

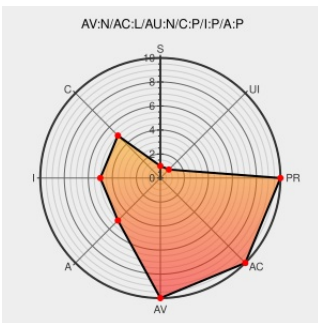
CVE-2004-1932

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

SQL injection vulnerability in (1) auth.php and (2) admin.php in PHP-Nuke 6.x through 7.2 allows remote attackers to execute arbitrary SQL code and create an administrator account via base64-encoded SQL in the admin parameter.

CVE-2004-1932 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](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF phpnuke-admin-bypass-authentication\(15835\)](#)

[waraxe-2004-SA#018] - Admin-level authentication bypass in phpnuke 6.x-7.2

[Exploit](#)
[Vendor Advisory](#)
www.waraxe.us
[text/html](#)

[MISC www.waraxe.us/index.php?modname=sa&id=18](http://www.waraxe.us/index.php?modname=sa&id=18)

'[waraxe-2004-SA#018 - Admin-level authentication bypass in' - MARC

marc.info
[text/html](#)

[BUGTRAQ 20040412 \[waraxe-2004-SA#018 - Admin-level authentication bypass in phpnuke 6.x-7.2\]](#)

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	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

```
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: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:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)