



CVE-2009-2288

Published on: 07/01/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:30 PM UTC

CVE-2009-2288

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Nagios](#) from [Nagios](#) contain the following vulnerability:

statuswml.cgi in Nagios before 3.1.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) ping or (2) Traceroute parameters.

CVE-2009-2288 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

HP Insight Control Suite For Linux Two Vulnerabilities - Secunia.com

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

[X](#) [SECUNIA 39227](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2010-0750](#)

Nagios "statuswml.cgi" Command Injection Vulnerability - Secunia
Advisories - Vulnerability Information - Secunia.com

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

[X](#) [SECUNIA 35543](#)

Nagios Enterprises · GitHub

[Exploit](#)
[tracker.nagios.org](#)
[text/html](#)

[CONFIRM](#)
[tracker.nagios.org/view.php?id=15](#)

Nagios - Nagios 3 Version History

[www.nagios.org](#)
[text/html](#)

[CONFIRM](#)
[www.nagios.org/development/history/core-3x/](#)

SecurityTracker.com Archives - Nagios Input Validation Flaw in 'statuswml.cgi' Lets Remote Users Execute Arbitrary Commands	www.securitytracker.com text/html	 SECTRACK 1022503
Ubuntu update for nagios2 and nagios3 - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 35688
Gentoo Linux Documentation -- Nagios: Execution of arbitrary code	security.gentoo.org text/html	 GENTOO GLSA-200907-15
'[security bulletin] HPSBMA02513 SSRT090110 rev.1 - Insight Control for Linux (IC-Linux) Remote Execu' - MARC	marc.info text/html	 HP SSRT090110
USN-795-1: Nagios vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-795-1
Debian update for nagios2 and nagios3 - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 35692
Debian -- Security Information -- DSA-1825-1 nagios2, nagios3	www.debian.org Depreciated Link text/html	 DEBIAN DSA-1825

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	Nagios	Nagios	1.0	All	All	All
Application	Nagios	Nagios	1.0b1	All	All	All
Application	Nagios	Nagios	1.0b2	All	All	All
Application	Nagios	Nagios	1.0b4	All	All	All
Application	Nagios	Nagios	1.1	All	All	All
Application	Nagios	Nagios	1.4.1	All	All	All
Application	Nagios	Nagios	2.0	All	All	All
Application	Nagios	Nagios	2.0b4	All	All	All
Application	Nagios	Nagios	2.10	All	All	All
Application	Nagios	Nagios	2.7	All	All	All
Application	Nagios	Nagios	3.0	All	All	All
Application	Nagios	Nagios	3.0	alpha1	All	All
Application	Nagios	Nagios	3.0	alpha2	All	All
Application	Nagios	Nagios	3.0	alpha3	All	All
Application	Nagios	Nagios	3.0	alpha4	All	All
Application	Nagios	Nagios	3.0	beta1	All	All

Application	Nagios	Nagios	3.0	beta2	All	All
Application	Nagios	Nagios	3.0	beta3	All	All
Application	Nagios	Nagios	3.0	beta4	All	All
Application	Nagios	Nagios	3.0	beta5	All	All
Application	Nagios	Nagios	3.0	beta6	All	All
Application	Nagios	Nagios	3.0	beta7	All	All
Application	Nagios	Nagios	3.0	rc1	All	All
Application	Nagios	Nagios	3.0	rc2	All	All
Application	Nagios	Nagios	3.0	rc3	All	All
Application	Nagios	Nagios	3.0.1	All	All	All
Application	Nagios	Nagios	3.0.2	All	All	All
Application	Nagios	Nagios	3.0.3	All	All	All
Application	Nagios	Nagios	3.0.4	All	All	All
Application	Nagios	Nagios	3.0.5	All	All	All
Application	Nagios	Nagios	3.0.6	All	All	All
Application	Nagios	Nagios	1.0	All	All	All
Application	Nagios	Nagios	1.0b1	All	All	All
Application	Nagios	Nagios	1.0b2	All	All	All
Application	Nagios	Nagios	1.0b4	All	All	All
Application	Nagios	Nagios	1.1	All	All	All
Application	Nagios	Nagios	1.4.1	All	All	All
Application	Nagios	Nagios	2.0	All	All	All
Application	Nagios	Nagios	2.0b4	All	All	All
Application	Nagios	Nagios	2.10	All	All	All
Application	Nagios	Nagios	2.7	All	All	All
Application	Nagios	Nagios	3.0	All	All	All
Application	Nagios	Nagios	3.0	alpha1	All	All
Application	Nagios	Nagios	3.0	alpha2	All	All
Application	Nagios	Nagios	3.0	alpha3	All	All
Application	Nagios	Nagios	3.0	alpha4	All	All
Application	Nagios	Nagios	3.0	beta1	All	All
Application	Nagios	Nagios	3.0	beta2	All	All
Application	Nagios	Nagios	3.0	beta3	All	All
Application	Nagios	Nagios	3.0	beta4	All	All
Application	Nagios	Nagios	3.0	beta5	All	All

Application	Nagios	Nagios	3.0	beta6	All	All
Application	Nagios	Nagios	3.0	beta7	All	All
Application	Nagios	Nagios	3.0	rc1	All	All
Application	Nagios	Nagios	3.0	rc2	All	All
Application	Nagios	Nagios	3.0	rc3	All	All
Application	Nagios	Nagios	3.0.1	All	All	All
Application	Nagios	Nagios	3.0.2	All	All	All
Application	Nagios	Nagios	3.0.3	All	All	All
Application	Nagios	Nagios	3.0.4	All	All	All
Application	Nagios	Nagios	3.0.5	All	All	All
Application	Nagios	Nagios	3.0.6	All	All	All
Application	Nagios	Nagios	All	All	All	All
cpe:2.3:a:nagios:nagios:1.0:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:1.0b1:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:1.0b2:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:1.0b4:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:1.1:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:1.4.1:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:2.0:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:2.0b4:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:2.10:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:2.7:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:alpha1:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:alpha2:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:alpha3:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:alpha4:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:beta1:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:beta2:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:beta3:*:*:*:*:*:						
cpe:2.3:a:nagios:nagios:3.0:beta4:*:*:*:*:*:						

```
cpe:2.3:a:nagios:nagios:3.0:beta5:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0:beta6:*. *. *. *. *. *
```

```
cpe:2.3:a:nagios:nagios:3.0:beta7:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0:rc3:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0.2:*:*:*:*:*:*:
```

cpe:2.3:a:nagios:nagios:3.0.3:*:*:*:*:*:*:

cpe:2.3:a:nagios:nagios:3.0.4:*:*:*:*:*:*:

cpe:2.3:a:nagios:nagios:3.0.5:*.:*:*:*:*:

```
cpe:2.3:a:nagios:nagios:3.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:1.0b1:::*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:1.0b2:::*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:1.0b4:::*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:1.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:nagios:nagios:1.4.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:2.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:2.0b4:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:2.10:*:*:*:*:*:*:
```

cpe:2.3:a:nagios:nagios:2.7:*:*:*:*:*:*:

cpe:2.3:a:nagios:nagios:3.0:*:*:*:*:*:*:

```
cpe:2.3:a:nagios:nagios:3.0:alpha1:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0:alpha2:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0:alpha3:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0:alpha4:*:*:*:*:*:
```

```
cpe:2.3:a:nagios:nagios:3.0:beta1:*. *. *. *. *. *
```

cpe:2.3:a:nagios:nagios:3.0:beta2:*****:
cpe:2.3:a:nagios:nagios:3.0:beta3:*****:
cpe:2.3:a:nagios:nagios:3.0:beta4:*****:
cpe:2.3:a:nagios:nagios:3.0:beta5:*****:
cpe:2.3:a:nagios:nagios:3.0:beta6:*****:
cpe:2.3:a:nagios:nagios:3.0:beta7:*****:
cpe:2.3:a:nagios:nagios:3.0:rc1:*****:
cpe:2.3:a:nagios:nagios:3.0:rc2:*****:
cpe:2.3:a:nagios:nagios:3.0:rc3:*****:
cpe:2.3:a:nagios:nagios:3.0.1:*****:
cpe:2.3:a:nagios:nagios:3.0.2:*****:
cpe:2.3:a:nagios:nagios:3.0.3:*****:
cpe:2.3:a:nagios:nagios:3.0.4:*****:
cpe:2.3:a:nagios:nagios:3.0.5:*****:
cpe:2.3:a:nagios:nagios:3.0.6:*****:
cpe:2.3:a:nagios:nagios:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© 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