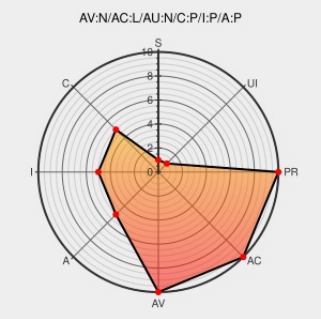
CVE-2009-2288

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
HP Insight Control Suite For Linux Two Vulnerabilities - Secunia.com	web.archive.org, text/html	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	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

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→