



CVE-2008-6373

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2008-6373
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-02 19:30:00 UTC
Updated	2017-08-17 01:29:00 UTC
Description	Unspecified vulnerability in Nagios before 3.0.6 has unspecified impact and remote attack vectors related to CGI programs,

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

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	1.0b3	All	All	All
Application	Nagios	Nagios	1.0b4	All	All	All
Application	Nagios	Nagios	1.0b5	All	All	All
Application	Nagios	Nagios	1.0b6	All	All	All
Application	Nagios	Nagios	1.0_b1	All	All	All
Application	Nagios	Nagios	1.0_b2	All	All	All
Application	Nagios	Nagios	1.0_b3	All	All	All
Application	Nagios	Nagios	1.1	All	All	All
Application	Nagios	Nagios	1.2	All	All	All
Application	Nagios	Nagios	1.3	All	All	All
Application	Nagios	Nagios	1.4	All	All	All
Application	Nagios	Nagios	1.4.1	All	All	All
Application	Nagios	Nagios	2.0	All	All	All
Application	Nagios	Nagios	2.0b1	All	All	All

Application	Nagios	Nagios	2.0b2	All	All	All
Application	Nagios	Nagios	2.0b3	All	All	All
Application	Nagios	Nagios	2.0b4	All	All	All
Application	Nagios	Nagios	2.0b5	All	All	All
Application	Nagios	Nagios	2.0b6	All	All	All
Application	Nagios	Nagios	2.0rc1	All	All	All
Application	Nagios	Nagios	2.0rc2	All	All	All
Application	Nagios	Nagios	2.1	All	All	All
Application	Nagios	Nagios	2.10	All	All	All
Application	Nagios	Nagios	2.11	All	All	All
Application	Nagios	Nagios	2.2	All	All	All
Application	Nagios	Nagios	2.3	All	All	All
Application	Nagios	Nagios	2.3.1	All	All	All
Application	Nagios	Nagios	2.4	All	All	All
Application	Nagios	Nagios	2.5	All	All	All
Application	Nagios	Nagios	2.7	All	All	All
Application	Nagios	Nagios	2.8	All	All	All
Application	Nagios	Nagios	2.9	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	1.0	All	All	All
Application	Nagios	Nagios	1.0b1	All	All	All
Application	Nagios	Nagios	1.0b2	All	All	All
Application	Nagios	Nagios	1.0b3	All	All	All
Application	Nagios	Nagios	1.0b4	All	All	All
Application	Nagios	Nagios	1.0b5	All	All	All
Application	Nagios	Nagios	1.0b6	All	All	All
Application	Nagios	Nagios	1.0_b1	All	All	All
Application	Nagios	Nagios	1.0_b2	All	All	All
Application	Nagios	Nagios	1.0_b3	All	All	All
Application	Nagios	Nagios	1.1	All	All	All
Application	Nagios	Nagios	1.2	All	All	All
Application	Nagios	Nagios	1.3	All	All	All
Application	Nagios	Nagios	1.4	All	All	All
Application	Nagios	Nagios	1.4.1	All	All	All
Application	Nagios	Nagios	2.0	All	All	All
Application	Nagios	Nagios	2.0b1	All	All	All
Application	Nagios	Nagios	2.0b2	All	All	All
Application	Nagios	Nagios	2.0b3	All	All	All
Application	Nagios	Nagios	2.0b4	All	All	All
Application	Nagios	Nagios	2.0b5	All	All	All
Application	Nagios	Nagios	2.0b6	All	All	All
Application	Nagios	Nagios	2.0rc1	All	All	All
Application	Nagios	Nagios	2.0rc2	All	All	All
Application	Nagios	Nagios	2.1	All	All	All
Application	Nagios	Nagios	2.10	All	All	All
Application	Nagios	Nagios	2.11	All	All	All
Application	Nagios	Nagios	2.2	All	All	All
Application	Nagios	Nagios	2.3	All	All	All
Application	Nagios	Nagios	2.3.1	All	All	All
Application	Nagios	Nagios	2.4	All	All	All
Application	Nagios	Nagios	2.5	All	All	All
Application	Nagios	Nagios	2.7	All	All	All
Application	Nagios	Nagios	2.8	All	All	All

Application	Nagios	Nagios	2.8	All	All	All
Application	Nagios	Nagios	2.9	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	All	All	All	All

References
Reference
HP Insight Control suite for Linux Bugs in Nagios Let Remote Users Conduct Cross-Site Request Forgery Attacks and Bypass Authentication
Webmail - OVH
Gentoo Linux Documentation -- Nagios: Execution of arbitrary code
Nagios External Commands and Adaptive Commands Unspecified Vulnerability
Nagios News - Nagios
HP Insight Control Suite For Linux Nagios Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
SSRT090060
Nagios Unspecified CGI Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com
IBM X-Force Exchange
Nagios: Nagios 3.x Version History
CVE Program record

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)