



CVE-2007-5803

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

Summary

CVE	CVE-2007-5803
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-05-13 23:20:00 UTC
Updated	2017-07-29 01:33:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in CGI programs in Nagios before 2.12 might allow remote attackers to injec

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.1	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	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	1.1	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

References			
Reference	Source	Link	Tags
[security-announce] SUSE Security Summary Report SUSE-SR:20078:011	SUSE	lists.opensuse.org	Exploit
Webmail OVH- OVH	VUPEN	www.vupen.com	
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	secunia.com	Vendor Adv
Nagios CGI Unspecified Cross-Site Scripting Vulnerability - Advisories - Secunia	SECUNIA	secunia.com	Vendor Adv
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Nagios Core download SourceForge.net	CONFIRM	sourceforge.net	
Nagios Unspecified Cross-Site Scripting Vulnerability	BID	www.securityfocus.com	
SourceForge.net: Files	CONFIRM	sourceforge.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

No vendor comments have been submitted for this CVE.

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