CVE-2012-6096

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-6096
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-01-22 23:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple stack-based buffer overflows in the get_history function in history.cgi in Nagios Core before 3.4.4, and Icinga 1.6.x

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Icinga	Icinga	1.6.0	All	All	All

Application	Icinga	Icinga	1.6.1	All	All	All
Application	Icinga	Icinga	1.7.0	All	All	All
Application	Icinga	Icinga	1.7.1	All	All	All
Application	Icinga	Icinga	1.7.2	All	All	All
Application	Icinga	Icinga	1.7.3	All	All	All
Application	Icinga	Icinga	1.8.0	All	All	All
Application	Icinga	Icinga	1.8.1	All	All	All
Application	Icinga	Icinga	1.8.2	All	All	All
Application	Icinga	Icinga	1.8.3	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	alpha5	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	3.1.0	All	All	All
Application	Nagios	Nagios	3.1.1	All	All	All
Application	Nagios	Nagios	3.1.2	All	All	All
Application	Nagios	Nagios	3.2.0	All	All	All
Application	Nagios	Nagios	3.2.1	All	All	All

Application	Nagios	Nagios	3.2.2	All	All	All
Application	Nagios	Nagios	3.2.3	All	All	All
Application	Nagios	Nagios	3.3.1	All	All	All
Application	Nagios	Nagios	3.4.0	All	All	All
Application	Nagios	Nagios	3.4.1	All	All	All
Application	Nagios	Nagios	3.4.2	All	All	All
Application	Nagios	Nagios	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Icinga 1.6.2, 1.7.4, 1.8.4 released | Icinga	af854a3a-2127
Debian -- Security Information -- DSA-2616-1 nagios3	af854a3a-2127
893269 – (CVE-2012-6096) CVE-2012-6096 nagios: stack-based buffer overflow in history.cgi	af854a3a-2127
Nagios history.cgi Remote Command Execution Vulnerability	af854a3a-2127
Nagios - Nagios Core 3.x Version History	af854a3a-2127
Nagios Core 'get_history()' Function Stack Based Buffer Overflow Vulnerability	af854a3a-2127
Nagios3 history.cgi Host Command Execution	af854a3a-2127
Debian -- Security Information -- DSA-2653-1 icinga	af854a3a-2127
openSUSE-SU-2013:0140-1: moderate: update for nagios	af854a3a-2127
Security Advisory SA51863 - Icinga history.cgi "show_history()" Buffer Overflow Vulnerability - Secunia	af854a3a-2127
www.osvdb.org/89170	af854a3a-2127
openSUSE-SU-2013:0169-1: moderate: update for icinga	af854a3a-2127
Bug #3532: CVE-2012-6096 - history.cgi remote command execution - Core, Classic UI, IDOUtils - Open Source Monitoring	af854a3a-2127
openSUSE-SU-2013:0206-1: moderate: update for icinga	af854a3a-2127
[Full-disclosure] Nagios Core 3.4.3: Stack based buffer overflow in web interface	af854a3a-2127
openSUSE-SU-2013:0188-1: moderate: update for nagios	af854a3a-2127
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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