



# CVE-2006-2489

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

## Summary

<b>CVE</b>	CVE-2006-2489
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-05-19 23:02:00 UTC
<b>Updated</b>	2018-10-03 21:41:00 UTC
<b>Description</b>	Integer overflow in CGI scripts in Nagios 1.x before 1.4.1 and 2.x before 2.3.1 allows remote attackers to cause a denial of service.

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b3	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b4	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b5	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b6	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.3	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.4	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b3	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b4	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b5	All	All	All

Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b6	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0rc1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0rc2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.3	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b3	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b4	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b5	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.0b6	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.3	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	1.4	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b3	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b4	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b5	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0b6	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0rc1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.0rc2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.1	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.2	All	All	All
Application	<a href="#">Nagios</a>	<a href="#">Nagios</a>	2.3	All	All	All

## References

Reference	Source	Link	Tag
Debian update for nagios - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
Debian -- Security Information -- DSA-1072-1 nagios	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
Secunia - Advisories - Nagios Content-Length Integer Overflow Vulnerability	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Pat
WordPress - Security - Content-Length Integer Overflow Vulnerability	WordPress		

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>	
USN-287-1: Nagios vulnerability   Ubuntu security notices	UBUNTU	<a href="http://usn.ubuntu.com">usn.ubuntu.com</a>	
Ubuntu update for nagios - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	
Gentoo Linux Documentation -- Nagios: Buffer overflow	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>	
Nagios Remote Content-Length Integer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
Nagios: Changelog	CONFIRM	<a href="http://www.nagios.org">www.nagios.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)