



CVE-2011-4963

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

Summary

CVE	CVE-2011-4963
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-07-26 19:55:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	nginx/Windows 1.3.x before 1.3.1 and 1.2.x before 1.2.1 allows remote attackers to bypass intended access restrictions and

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Nginx	All	All	All	All

Application	F5	Nginx	1.3.0	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference	Source		Link	Tags		
[nginx-announce] security advisory	af854a3a-2127-422b-91ae-364da2661108		mailman.nginx.org	Mitigation, Vendor Advisory		
nginx security advisories	af854a3a-2127-422b-91ae-364da2661108		nginx.org	Vendor Advisory		
404 Not Found	af854a3a-2127-422b-91ae-364da2661108		english.securitylab.ru	Mitigation, Third Party Advisory		
CVE Program record	CVE.ORG		www.cve.org	canonical		
NVD vulnerability detail	NVD		nvd.nist.gov	canonical, analysis		
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