CVE-2010-2263

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

Summary

CVE	CVE-2010-2263
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-15 14:04:24 UTC
Updated	2026-04-29 01:13:23 UTC
Description	nginx 0.8 before 0.8.40 and 0.7 before 0.7.66, when running on Windows, allows remote attackers to obtain source code or

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: CWE-200 | 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	All	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
:::::0th3r ****ing S3Cbl0g:::: Only 4 Fun & pr0fit ;): :::FULL & RESPONSIBLE DISCLOSURE:::NGINX [ENGINE X] SERVER <= 0.7.65 /0.8.39
Nginx <= 0.7.65 / 0.8.39 (dev) Source Disclosure / Download Vulnerability
nginx Remote Source Code Disclosure and Denial of Service Vulnerabilities
Nginx 0.8.36 Source Disclosure and DoS Vulnerabilities
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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