CVE-2016-1247

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

Summary

CVE	CVE-2016-1247
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-29 17:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The nginx package before 1.6.2-5+deb8u3 on Debian jessie, the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.100690000 probability, percentile 0.931400000 (date 2026-05-09)

Problem Types: CWE-59 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	F5	Nginx	All	All	All	All
Application	F5	Nginx	All	All	All	All
Application	F5	Nginx	All	All	All	All
Application	F5	Nginx	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
NGINX: Privilege escalation (GLSA 201701-22) — Gentoo security	af854a3a-2127-422b-91ae-3
EP 1. G1VE M3 R00T | CVE 2016-1247 - YouTube	af854a3a-2127-422b-91ae-3
Nginx Root Privilege Escalation ≈ Packet Storm	af854a3a-2127-422b-91ae-3
[SECURITY] Fedora 34 Update: nginx-1.20.0-2.fc34 - package-announce - Fedora Mailing-Lists	af854a3a-2127-422b-91ae-3
Debian -- Security Information -- DSA-3701-1 nginx	af854a3a-2127-422b-91ae-3
Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247	af854a3a-2127-422b-91ae-3
USN-3114-1: nginx vulnerability | Ubuntu	af854a3a-2127-422b-91ae-3
nginx on Debian Log File Permissions Let Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-91ae-3
Full Disclosure: Nginx (Debian-based distros) - Root Privilege Escalation Vulnerability (CVE-2016-1247)	af854a3a-2127-422b-91ae-3
SecurityFocus	af854a3a-2127-422b-91ae-3
Nginx CVE-2016-1247 Remote Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-3
[SECURITY] Fedora 33 Update: nginx-1.20.0-2.fc33 - package-announce - Fedora Mailing-Lists	af854a3a-2127-422b-91ae-3
[SECURITY] Fedora 32 Update: nginx-1.20.0-2.fc32 - package-announce - Fedora Mailing-Lists	af854a3a-2127-422b-91ae-3
Nginx (Debian-Based + Gentoo) - 'logrotate' Local Privilege Escalation	af854a3a-2127-422b-91ae-3
Full Disclosure: Nginx (Debian-based + Gentoo distros) - Root Privilege Escalation [CVE-2016-1247 UPDATE]	af854a3a-2127-422b-91ae-3
[SECURITY] Fedora 33 Update: nginx-1.20.0-2.fc33 - package-announce - Fedora Mailing-Lists	MITRE
[SECURITY] Fedora 32 Update: nginx-1.20.0-2.fc32 - package-announce - Fedora Mailing-Lists	MITRE
[SECURITY] Fedora 34 Update: nginx-1.20.0-2.fc34 - package-announce - Fedora Mailing-Lists	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

281277 Fedora Security Update for nginx (FEDORA-2021-3aa9ac7fd1)

281278 Fedora Security Update for nginx (FEDORA-2021-1556d440ba)

281279 Fedora Security Update for nginx (FEDORA-2021-10c1cd4cba)

356191 Amazon Linux Security Advisory for nginx : ALASNGINX1-2023-005

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**