



CVE-2016-0771

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

Summary

CVE	CVE-2016-0771
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-13 22:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The internal DNS server in Samba 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6, and 4.4.x before 4.4.0rc4, when

Risk And Classification

Primary CVSS: v3.0 5.9 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H
2.0	nvd@nist.gov	Primary	4.9		AV:N/AC:M/Au:S/C:P/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

High

CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Partial

Integrity

None

Availability

Partial

AV:N/AC:M/Au:S/C:P/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	4.0.0	All	All	All
Application	Samba	Samba	4.0.1	All	All	All
Application	Samba	Samba	4.0.10	All	All	All
Application	Samba	Samba	4.0.11	All	All	All
Application	Samba	Samba	4.0.12	All	All	All
Application	Samba	Samba	4.0.13	All	All	All
Application	Samba	Samba	4.0.14	All	All	All
Application	Samba	Samba	4.0.15	All	All	All
Application	Samba	Samba	4.0.16	All	All	All
Application	Samba	Samba	4.0.17	All	All	All
Application	Samba	Samba	4.0.18	All	All	All
Application	Samba	Samba	4.0.19	All	All	All
Application	Samba	Samba	4.0.2	All	All	All
Application	Samba	Samba	4.0.20	All	All	All
Application	Samba	Samba	4.0.21	All	All	All
Application	Samba	Samba	4.0.22	All	All	All
Application	Samba	Samba	4.0.23	All	All	All

Application	Samba	Samba	4.0.24	All	All	All
Application	Samba	Samba	4.0.3	All	All	All
Application	Samba	Samba	4.0.4	All	All	All
Application	Samba	Samba	4.0.5	All	All	All
Application	Samba	Samba	4.0.6	All	All	All
Application	Samba	Samba	4.0.7	All	All	All
Application	Samba	Samba	4.0.8	All	All	All
Application	Samba	Samba	4.0.9	All	All	All
Application	Samba	Samba	4.1.0	All	All	All
Application	Samba	Samba	4.1.1	All	All	All
Application	Samba	Samba	4.1.10	All	All	All
Application	Samba	Samba	4.1.11	All	All	All
Application	Samba	Samba	4.1.12	All	All	All
Application	Samba	Samba	4.1.13	All	All	All
Application	Samba	Samba	4.1.14	All	All	All
Application	Samba	Samba	4.1.15	All	All	All
Application	Samba	Samba	4.1.16	All	All	All
Application	Samba	Samba	4.1.17	All	All	All
Application	Samba	Samba	4.1.18	All	All	All
Application	Samba	Samba	4.1.19	All	All	All
Application	Samba	Samba	4.1.2	All	All	All
Application	Samba	Samba	4.1.20	All	All	All
Application	Samba	Samba	4.1.21	All	All	All
Application	Samba	Samba	4.1.22	All	All	All
Application	Samba	Samba	4.1.3	All	All	All
Application	Samba	Samba	4.1.4	All	All	All
Application	Samba	Samba	4.1.5	All	All	All
Application	Samba	Samba	4.1.6	All	All	All
Application	Samba	Samba	4.1.7	All	All	All
Application	Samba	Samba	4.1.8	All	All	All
Application	Samba	Samba	4.1.9	All	All	All
Application	Samba	Samba	4.2.0	rc1	All	All
Application	Samba	Samba	4.2.0	rc2	All	All
Application	Samba	Samba	4.2.0	rc3	All	All
Application	Samba	Samba	4.2.0	rc4	All	All
Application	Samba	Samba	4.2.0	All	All	All

Application	Samba	Samba	4.2.1	All	All	All
Application	Samba	Samba	4.2.2	All	All	All
Application	Samba	Samba	4.2.3	All	All	All
Application	Samba	Samba	4.2.4	All	All	All
Application	Samba	Samba	4.2.5	All	All	All
Application	Samba	Samba	4.2.6	All	All	All
Application	Samba	Samba	4.2.7	All	All	All
Application	Samba	Samba	4.2.8	All	All	All
Application	Samba	Samba	4.3.0	All	All	All
Application	Samba	Samba	4.3.1	All	All	All
Application	Samba	Samba	4.3.2	All	All	All
Application	Samba	Samba	4.3.3	All	All	All
Application	Samba	Samba	4.3.4	All	All	All
Application	Samba	Samba	4.3.5	All	All	All
Application	Samba	Samba	4.4.0	rc1	All	All
Application	Samba	Samba	4.4.0	rc2	All	All
Application	Samba	Samba	4.4.0	rc3	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Samba Out-of-Bounds Read Error Lets Remote Users Deny Service or Obtain Potentially Sensitive Information - SecurityTracker	af854a3a-
Debian -- Security Information -- DSA-3514-1 samba	af854a3a-
Samba CVE-2016-0771 Out of Bound Read Denial of Service Vulnerability	af854a3a-
USN-2922-1: Samba vulnerabilities Ubuntu	af854a3a-
Access Denied	af854a3a-
Samba - Security Announcement Archive	af854a3a-
Bug 11128 – ndr_push_error unexpected blob length is too large	af854a3a-
[security-announce] openSUSE-SU-2016:0813-1: important: Security update	af854a3a-
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.

© [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](#)