



# CVE-2016-2113

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

| Summary         |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-2113                                                                                                                |
| State           | PUBLISHED                                                                                                                    |
| Assigner        | redhat                                                                                                                       |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                 |
| Published       | 2016-04-25 00:59:03 UTC                                                                                                      |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                      |
| Description     | Samba 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not verify X.509 certificates from TLS servers, whi |

Risk And Classification

Primary CVSS: v3.0 7.4 HIGH from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.0     | nvd@nist.gov | Primary | 7.4   | HIGH     | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N |
| 2.0     | nvd@nist.gov | Primary | 5.8   |          | AV:N/AC:M/Au:N/C:P/I:P/A:N                   |

| CVSS v3.0 Breakdown |           |
|---------------------|-----------|
| Attack Vector       | Network   |
| Attack Complexity   | High      |
| Privileges Required | None      |
| User Interaction    | None      |
| Scope               | Unchanged |
| Confidentiality     | High      |
| Integrity           | High      |
| Availability        |           |

None

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

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

## 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 | 15.10   | All    | All     | All      |
| Operating System | Canonical | Ubuntu Linux | 16.04   | All    | All     | All      |
| 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 | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.21 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.22 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.23 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.24 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.25 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.26 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.3  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.4  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.5  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.6  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.7  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.8  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.0.9  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.0  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.1  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.10 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.11 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.12 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.13 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.14 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.15 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.16 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.17 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.18 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.19 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.2  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.20 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.21 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.22 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.23 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.3  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.4  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.5  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.6  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.7  | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.8  | All | All | All |

|             |                       |                       |       |     |     |     |
|-------------|-----------------------|-----------------------|-------|-----|-----|-----|
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.8 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.1.9 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.0 | rc1 | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.0 | rc2 | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.0 | rc3 | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.0 | rc4 | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.1 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.2 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.3 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.4 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.5 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.6 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.7 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.8 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.2.9 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.3.0 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.3.1 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.3.2 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.3.3 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.3.4 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.3.5 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.3.6 | All | All | All |
| Application | <a href="#">Samba</a> | <a href="#">Samba</a> | 4.4.0 | All | All | All |

|                                   |                    |                     |              |  |               |  |
|-----------------------------------|--------------------|---------------------|--------------|--|---------------|--|
| Vendor Declared Affected Products |                    |                     |              |  |               |  |
| Source                            | Vendor             | Product             | Version      |  | Platforms     |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a |  | Not specified |  |

|                                                                         |
|-------------------------------------------------------------------------|
| References                                                              |
| Reference                                                               |
| Badlock Bug                                                             |
| Red Hat Customer Portal                                                 |
| Red Hat Customer Portal                                                 |
| Broadcom Support Portal                                                 |
| USN-2950-1: Samba vulnerabilities   Ubuntu                              |
| [security-announce] openSUSE-SU-2016:1064-1: important: Security update |
| Samba - Release Notes Archive                                           |

|                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------|
| Samba - Release Notes Archive                                                                                                          |
| [security-announce] SUSE-SU-2016:1023-1: important: Security update for                                                                |
| [SECURITY] Fedora 23 Update: samba-4.3.8-0.fc23                                                                                        |
| USN-2950-2: libsoup update   Ubuntu                                                                                                    |
| Samba: Multiple vulnerabilities (GLSA 201612-47) — Gentoo security                                                                     |
| USN-2950-5: Samba regression   Ubuntu                                                                                                  |
| [security-announce] openSUSE-SU-2016:1025-1: important: Security update                                                                |
| [security-announce] SUSE-SU-2016:1024-1: important: Security update for                                                                |
| The Slackware Linux Project: Slackware Security Advisories                                                                             |
| [security-announce] SUSE-SU-2016:1022-1: important: Security update for                                                                |
| Samba - Security Announcement Archive                                                                                                  |
| [SECURITY] Fedora 22 Update: samba-4.2.11-0.fc22                                                                                       |
| Red Hat Customer Portal                                                                                                                |
| Red Hat Customer Portal                                                                                                                |
| [security-announce] openSUSE-SU-2016:1107-1: important: Security update                                                                |
| Oracle Linux Bulletin - April 2016                                                                                                     |
| USN-2950-3: Samba regressions   Ubuntu                                                                                                 |
| Samba Multiple Flaws Let Remote Users Hijack Connections, Obtain Potentially Sensitive Information, and Deny Service - SecurityTracker |
| Samba - Latest News                                                                                                                    |
| USN-2950-4: Samba regressions   Ubuntu                                                                                                 |
| [security-announce] openSUSE-SU-2016:1106-1: important: Security update                                                                |
| [SECURITY] Fedora 24 Update: samba-4.4.2-1.fc24                                                                                        |
| [security-announce] SUSE-SU-2016:1028-1: important: Security update for                                                                |
| Debian -- Security Information -- DSA-3548-1 samba                                                                                     |
| 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.

[site](#). This site includes MITRE data granted under the following [license](#).

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

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