



# CVE-2017-15275

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

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-15275                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2017-11-27 22:29:00 UTC                                                                                                        |
| <b>Updated</b>         | 2022-08-29 20:43:00 UTC                                                                                                        |
| <b>Description</b>     | Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear s |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                                  | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>             | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>             | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>             | 17.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>             | 17.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>             | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>             | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>             | 17.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>             | 17.10   | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a>             | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a>             | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a>             | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a>             | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>    | <a href="#">Enterprise Linux Desktop</a> | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>    | <a href="#">Enterprise Linux Desktop</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>    | <a href="#">Enterprise Linux Desktop</a> | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>    | <a href="#">Enterprise Linux Desktop</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>    | <a href="#">Enterprise Linux Server</a>  | 6.0     | All    | All     | All      |

|                  |                        |                                              |     |     |     |     |
|------------------|------------------------|----------------------------------------------|-----|-----|-----|-----|
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 7.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 7.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 7.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 7.0 | All | All | All |
| Application      | <a href="#">Samba</a>  | <a href="#">Samba</a>                        | All | All | All | All |
| Application      | <a href="#">Samba</a>  | <a href="#">Samba</a>                        | All | All | All | All |

References

| Reference                                                                                                                     | Source    |
|-------------------------------------------------------------------------------------------------------------------------------|-----------|
| Red Hat Customer Portal                                                                                                       | REDHAT    |
| Samba - Security Announcement Archive                                                                                         | CONFIRMED |
| Document Display   HPE Support Center                                                                                         | CONFIRMED |
| Red Hat Customer Portal                                                                                                       | REDHAT    |
| USN-3486-2: Samba vulnerability   Ubuntu                                                                                      | UBUNTU    |
| Red Hat Customer Portal                                                                                                       | REDHAT    |
| [SECURITY] [DLA 1183-1] samba security update                                                                                 | MLIST     |
| Samba CVE-2017-15275 Information Disclosure Vulnerability                                                                     | BID       |
| Samba Flaw Lets Remote Users Obtain Potentially Sensitive Information from Heap Memory on the Target System - SecurityTracker | SECT      |
| USN-3486-1: Samba vulnerabilities   Ubuntu                                                                                    | UBUNTU    |
| Synology Inc.                                                                                                                 | CONFIRMED |
| Debian -- Security Information -- DSA-4043-1 samba                                                                            | DEBIAN    |
| Samba: Multiple vulnerabilities (GLSA 201805-07) — Gentoo Security                                                            | GENTOO    |
| CVE Program record                                                                                                            | CVE.COM   |
| NVD vulnerability detail                                                                                                      | NVD       |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

|                                                               |
|---------------------------------------------------------------|
| <a href="#">500633</a> Alpine Linux Security Update for samba |
| <a href="#">504397</a> Alpine Linux Security Update for samba |

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](https://cve.report/api)

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