



CVE-2015-0240

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

Summary

CVE	CVE-2015-0240
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-24 01:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Netlogon server implementation in smbd in Samba 3.5.x and 3.6.x before 3.6.25, 4.0.x before 4.0.25, 4.1.x before 4.1.1

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

Problem Types: CWE-17 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/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	12.04	All	All	All

Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Samba	Samba	3.5.0	All	All	All
Application	Samba	Samba	3.5.1	All	All	All
Application	Samba	Samba	3.5.10	All	All	All
Application	Samba	Samba	3.5.11	All	All	All
Application	Samba	Samba	3.5.12	All	All	All
Application	Samba	Samba	3.5.13	All	All	All
Application	Samba	Samba	3.5.14	All	All	All
Application	Samba	Samba	3.5.15	All	All	All
Application	Samba	Samba	3.5.16	All	All	All
Application	Samba	Samba	3.5.17	All	All	All
Application	Samba	Samba	3.5.18	All	All	All
Application	Samba	Samba	3.5.19	All	All	All
Application	Samba	Samba	3.5.2	All	All	All
Application	Samba	Samba	3.5.20	All	All	All
Application	Samba	Samba	3.5.21	All	All	All
Application	Samba	Samba	3.5.22	All	All	All
Application	Samba	Samba	3.5.3	All	All	All
Application	Samba	Samba	3.5.4	All	All	All
Application	Samba	Samba	3.5.5	All	All	All
Application	Samba	Samba	3.5.6	All	All	All
Application	Samba	Samba	3.5.7	All	All	All
Application	Samba	Samba	3.5.8	All	All	All
Application	Samba	Samba	3.5.9	All	All	All
Application	Samba	Samba	3.6.0	All	All	All
Application	Samba	Samba	3.6.1	All	All	All
Application	Samba	Samba	3.6.10	All	All	All
Application	Samba	Samba	3.6.11	All	All	All
Application	Samba	Samba	3.6.12	All	All	All

Application	Samba	Samba	3.6.13	All	All	All
Application	Samba	Samba	3.6.14	All	All	All
Application	Samba	Samba	3.6.15	All	All	All
Application	Samba	Samba	3.6.16	All	All	All
Application	Samba	Samba	3.6.17	All	All	All
Application	Samba	Samba	3.6.18	All	All	All
Application	Samba	Samba	3.6.19	All	All	All
Application	Samba	Samba	3.6.2	All	All	All
Application	Samba	Samba	3.6.20	All	All	All
Application	Samba	Samba	3.6.21	All	All	All
Application	Samba	Samba	3.6.22	All	All	All
Application	Samba	Samba	3.6.23	All	All	All
Application	Samba	Samba	3.6.24	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	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	4.1.2	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

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

References
Reference
Samba: Multiple vulnerabilities (GLSA 201502-15) — Gentoo security
USN-2508-1: Samba vulnerability Ubuntu
Red Hat Customer Portal
Red Hat Customer Portal
Samba vulnerability (CVE-2015-0240) - Red Hat Customer Portal

[security-announce] SUSE-SU-2015:0386-1: important: Security update for
Red Hat Customer Portal
[security-announce] openSUSE-SU-2016:1064-1: important: Security update
Support / Security / Advisories // MDVSA-2015:082 Mandriva
Oracle Bulletin Board Update - January 2015
Mageia Advisory: MGASA-2015-0084 - Updated samba packages fix CVE-2015-0240
Samba vulnerability (CVE-2015-0240) Red Hat Security
Red Hat Customer Portal
Red Hat Customer Portal
'[security bulletin] HPSBUX03320 SSRT101952 rev.1 - HP-UX CIFS Server (Samba), Remote Denial of Servi' - MARC
[security-announce] openSUSE-SU-2015:0375-1: important: Security update
The Slackware Linux Project: Slackware Security Advisories
[security-announce] SUSE-SU-2015:0371-1: important: Security update for
Debian -- Security Information -- DSA-3171-1 samba
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability
Red Hat Customer Portal
Red Hat Customer Portal
Samba smbd Memory Free Error Lets Remote Users Execute Arbitrary Code with Root Privileges - SecurityTracker
Support / Security / Advisories // MDVSA-2015:081 Mandriva
'[security bulletin] HPSBGN03288 rev.1 - HP Server Automation, Remote Arbitrary Code Execution' - MARC
Red Hat Customer Portal
Red Hat Customer Portal
Samba < 3.6.2 (x86) - Denial of Service (PoC) - Linux_x86 dos Exploit
[security-announce] openSUSE-SU-2016:1107-1: important: Security update
Samba Remote Code Execution Vulnerability - Lenovo Support US
Samba - Security Announcement Archive
Samba Remote Code Execution Vulnerability - Lenovo Support (US)
security.netapp.com/advisory/ntap-20250509-0001
[security-announce] openSUSE-SU-2016:1106-1: important: Security update
1191325 – (CVE-2015-0240) CVE-2015-0240 samba: talloc free on uninitialized stack pointer in netlogon server could lead to remote-code ex
[security-announce] SUSE-SU-2015:0353-1: important: Security update for
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal

Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
CVE-2015-0240 - Red Hat Customer Portal
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.