



CVE-2012-1182

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

Summary

CVE	CVE-2012-1182
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-10 21:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The RPC code generator in Samba 3.x before 3.4.16, 3.5.x before 3.5.14, and 3.6.x before 3.6.4 does not implement valida

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-189 | 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
Application	Samba	Samba	3.0.0	All	All	All

Application	Samba	Samba	3.0.1	All	All	All
Application	Samba	Samba	3.0.10	All	All	All
Application	Samba	Samba	3.0.11	All	All	All
Application	Samba	Samba	3.0.12	All	All	All
Application	Samba	Samba	3.0.13	All	All	All
Application	Samba	Samba	3.0.14	All	All	All
Application	Samba	Samba	3.0.14	a	All	All
Application	Samba	Samba	3.0.14a	All	All	All
Application	Samba	Samba	3.0.15	All	All	All
Application	Samba	Samba	3.0.16	All	All	All
Application	Samba	Samba	3.0.17	All	All	All
Application	Samba	Samba	3.0.18	All	All	All
Application	Samba	Samba	3.0.19	All	All	All
Application	Samba	Samba	3.0.2	All	All	All
Application	Samba	Samba	3.0.2	a	All	All
Application	Samba	Samba	3.0.20	All	All	All
Application	Samba	Samba	3.0.20	a	All	All
Application	Samba	Samba	3.0.20	b	All	All
Application	Samba	Samba	3.0.20a	All	All	All
Application	Samba	Samba	3.0.20b	All	All	All
Application	Samba	Samba	3.0.21	All	All	All
Application	Samba	Samba	3.0.21	a	All	All
Application	Samba	Samba	3.0.21	b	All	All
Application	Samba	Samba	3.0.21	c	All	All
Application	Samba	Samba	3.0.21a	All	All	All
Application	Samba	Samba	3.0.21b	All	All	All
Application	Samba	Samba	3.0.21c	All	All	All
Application	Samba	Samba	3.0.22	All	All	All
Application	Samba	Samba	3.0.23	All	All	All
Application	Samba	Samba	3.0.23	a	All	All
Application	Samba	Samba	3.0.23	b	All	All
Application	Samba	Samba	3.0.23	c	All	All
Application	Samba	Samba	3.0.23	d	All	All
Application	Samba	Samba	3.0.23a	All	All	All
Application	Samba	Samba	3.0.23b	All	All	All
Application	Samba	Samba	3.0.23c	All	All	All

Application	Samba	Samba	3.0.23d	All	All	All
Application	Samba	Samba	3.0.24	All	All	All
Application	Samba	Samba	3.0.25	All	All	All
Application	Samba	Samba	3.0.25	a	All	All
Application	Samba	Samba	3.0.25	b	All	All
Application	Samba	Samba	3.0.25	c	All	All
Application	Samba	Samba	3.0.25	pre1	All	All
Application	Samba	Samba	3.0.25	pre2	All	All
Application	Samba	Samba	3.0.25	rc1	All	All
Application	Samba	Samba	3.0.25	rc2	All	All
Application	Samba	Samba	3.0.25	rc3	All	All
Application	Samba	Samba	3.0.25a	All	All	All
Application	Samba	Samba	3.0.25b	All	All	All
Application	Samba	Samba	3.0.25c	All	All	All
Application	Samba	Samba	3.0.26	All	All	All
Application	Samba	Samba	3.0.26	a	All	All
Application	Samba	Samba	3.0.26a	All	All	All
Application	Samba	Samba	3.0.27	All	All	All
Application	Samba	Samba	3.0.27	a	All	All
Application	Samba	Samba	3.0.28	All	All	All
Application	Samba	Samba	3.0.28	a	All	All
Application	Samba	Samba	3.0.29	All	All	All
Application	Samba	Samba	3.0.2a	All	All	All
Application	Samba	Samba	3.0.3	All	All	All
Application	Samba	Samba	3.0.30	All	All	All
Application	Samba	Samba	3.0.31	All	All	All
Application	Samba	Samba	3.0.32	All	All	All
Application	Samba	Samba	3.0.33	All	All	All
Application	Samba	Samba	3.0.34	All	All	All
Application	Samba	Samba	3.0.35	All	All	All
Application	Samba	Samba	3.0.36	All	All	All
Application	Samba	Samba	3.0.37	All	All	All
Application	Samba	Samba	3.0.4	All	All	All
Application	Samba	Samba	3.0.4	rc1	All	All
Application	Samba	Samba	3.0.5	All	All	All

Application	Samba	Samba	3.0.6	All	All	All
Application	Samba	Samba	3.0.7	All	All	All
Application	Samba	Samba	3.0.8	All	All	All
Application	Samba	Samba	3.0.9	All	All	All
Application	Samba	Samba	3.1.0	All	All	All
Application	Samba	Samba	3.2.0	All	All	All
Application	Samba	Samba	3.2.1	All	All	All
Application	Samba	Samba	3.2.10	All	All	All
Application	Samba	Samba	3.2.11	All	All	All
Application	Samba	Samba	3.2.12	All	All	All
Application	Samba	Samba	3.2.13	All	All	All
Application	Samba	Samba	3.2.14	All	All	All
Application	Samba	Samba	3.2.15	All	All	All
Application	Samba	Samba	3.2.2	All	All	All
Application	Samba	Samba	3.2.3	All	All	All
Application	Samba	Samba	3.2.4	All	All	All
Application	Samba	Samba	3.2.5	All	All	All
Application	Samba	Samba	3.2.6	All	All	All
Application	Samba	Samba	3.2.7	All	All	All
Application	Samba	Samba	3.2.8	All	All	All
Application	Samba	Samba	3.2.9	All	All	All
Application	Samba	Samba	3.3.0	All	All	All
Application	Samba	Samba	3.3.1	All	All	All
Application	Samba	Samba	3.3.10	All	All	All
Application	Samba	Samba	3.3.11	All	All	All
Application	Samba	Samba	3.3.12	All	All	All
Application	Samba	Samba	3.3.13	All	All	All
Application	Samba	Samba	3.3.14	All	All	All
Application	Samba	Samba	3.3.15	All	All	All
Application	Samba	Samba	3.3.16	All	All	All
Application	Samba	Samba	3.3.2	All	All	All
Application	Samba	Samba	3.3.3	All	All	All
Application	Samba	Samba	3.3.4	All	All	All
Application	Samba	Samba	3.3.5	All	All	All
Application	Samba	Samba	3.3.6	All	All	All
Application	Samba	Samba	3.3.7	All	All	All

Application	Samba	Samba	3.3.7	All	All	All
Application	Samba	Samba	3.3.8	All	All	All
Application	Samba	Samba	3.3.9	All	All	All
Application	Samba	Samba	3.4.0	All	All	All
Application	Samba	Samba	3.4.1	All	All	All
Application	Samba	Samba	3.4.10	All	All	All
Application	Samba	Samba	3.4.11	All	All	All
Application	Samba	Samba	3.4.12	All	All	All
Application	Samba	Samba	3.4.13	All	All	All
Application	Samba	Samba	3.4.14	All	All	All
Application	Samba	Samba	3.4.2	All	All	All
Application	Samba	Samba	3.4.3	All	All	All
Application	Samba	Samba	3.4.4	All	All	All
Application	Samba	Samba	3.4.5	All	All	All
Application	Samba	Samba	3.4.6	All	All	All
Application	Samba	Samba	3.4.7	All	All	All
Application	Samba	Samba	3.4.8	All	All	All
Application	Samba	Samba	3.4.9	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	3.5.2	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	3.6.2	All	All	All
Application	Samba	Samba	3.6.3	All	All	All

Application	Samba	Samba	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	N/a	affected n/a		Not specified	
References						
Reference					Source	
About Secunia Research Flexera					af854a3a-2127-422	
About Secunia Research Flexera					af854a3a-2127-422	
[SECURITY] Fedora 17 Update: samba-3.6.4-82.fc17.1					af854a3a-2127-422	
[SECURITY] Fedora 16 Update: samba4-4.0.0-38.alpha16.fc16					af854a3a-2127-422	
About Secunia Research Flexera					af854a3a-2127-422	
[SECURITY] Fedora 15 Update: samba-3.5.14-73.fc15.1					af854a3a-2127-422	
Samba - Release Notes Archive					af854a3a-2127-422	
[security-announce] SUSE-SU-2012:0504-1: critical: Security update for S					af854a3a-2127-422	
USN-1423-1: Samba vulnerability Ubuntu					af854a3a-2127-422	
Security Advisory SA48754 - Red Hat update for samba3x - Secunia					af854a3a-2127-422	
About the security content of OS X Lion v10.7.4 and Security Update 2012-002					af854a3a-2127-422	
[security-announce] SUSE-SU-2012:0501-1: critical: Security update for S					af854a3a-2127-422	
'[security bulletin] HPSBUX02789 SSRT100824 rev.3 - HP-UX CIFS Server (Samba), Remote Execution of Ar' - MARC					af854a3a-2127-422	
[SECURITY] Fedora 16 Update: samba-3.6.4-82.fc16					af854a3a-2127-422	
Security Advisory SA48818 - Debian update for samba - Secunia					af854a3a-2127-422	
Security Advisory SA48873 - SUSE update for samba - Secunia					af854a3a-2127-422	
mandriva.com					af854a3a-2127-422	
[security-announce] SUSE-SU-2012:0515-1: critical: Security update for S					af854a3a-2127-422	
[security-announce] SUSE-SU-2012:0502-1: critical: Security update for S					af854a3a-2127-422	
Samba Buffer Overflow in NDR Marshalling Code Lets Remote Users Execute Arbitrary Code - SecurityTracker					af854a3a-2127-422	
APPLE-SA-2012-05-09-1 OS X Lion v10.7.4 and Security Update 2012-002					af854a3a-2127-422	
'[security bulletin] HPSBMU02790 SSRT100872 rev.1 - HP Server Automation, Remote Execution of Arbitra' - MARC					af854a3a-2127-422	
Security Alerts - Secunia					af854a3a-2127-422	
About Secunia Research Flexera					af854a3a-2127-422	
Debian -- Security Information -- DSA-2450-1 samba					af854a3a-2127-422	
Collax					af854a3a-2127-422	
Samba - Security Announcement Archive					af854a3a-2127-422	
CVE Program record					CVE.ORG	

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](#)