CVE-2016-2118

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

Summary

CVE	CVE-2016-2118
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-12 23:59:37 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The MS-SAMR and MS-LSAD protocol implementations in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x b

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Problem Types: CWE-254 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Badlock Bug
Red Hat Customer Portal
Red Hat Customer Portal
Samba CVE-2016-2118 Man in the Middle Security Bypass Vulnerability
Red Hat Customer Portal
Public KB - SA40196 - [Pulse Secure] Badlock security advisory (CVE-2016-2118)
Red Hat Customer Portal
StruxureWare Data Center Operation Software Vulnerability Fixes - User Assistance for StruxureWare Data Center Operation 8 - Help Center
Broadcom Support Portal
USN-2950-1: Samba vulnerabilities | Ubuntu

[security-announce] openSUSE-SU-2016:1064-1: important: Security update

Vulnerability Note VU#813296 - Microsoft Windows and Samba may allow spoofing of authenticated users ("Badlock")

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

Red Hat Customer Portal

Red Hat Customer Portal

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

Badlock Security flaw in Samba - CVE-2016-2118 - Red Hat Customer Portal

Document Display | HPE Support Center

The Slackware Linux Project: Slackware Security Advisories

Red Hat Customer Portal

[security-announce] SUSE-SU-2016:1022-1: important: Security update for

[SECURITY] Fedora 22 Update: samba-4.2.11-0.fc22

Document Display | HPE Support Center

Red Hat Customer Portal

Red Hat Customer Portal

Page not found - NetApp Knowledgebase

Red Hat Customer Portal

Red Hat Customer Portal

[security-announce] openSUSE-SU-2016:1107-1: important: Security update

Samba - Security Announcement Archive

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**