CVE-2013-4476

Published on: 11/13/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:27 PM UTC

CVE-2013-4476

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF

Certain versions of Samba from Samba contain the following vulnerability:

Samba 4.0.x before 4.0.11 and 4.1.x before 4.1.1, when LDAP or HTTP is provided over SSL, uses world-readable permissions for a private key, which allows local users to obtain sensitive information by reading the key file, as demonstrated by access to the local filesystem on an AD domain controller.

CVE-2013-4476 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 1.2 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Samba: Multiple vulnerabilities (GLSA 201502-15) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201502-15
Samba - Security Announcement Archive	Vendor Advisory www.samba.org text/html	CONFIRM www.samba.org/samba/security/CVE-2013-4476
Samba - Release Notes Archive	www.samba.org text/html	CONFIRM www.samba.org/samba/history/samba-4.1.1.html
Samba - Release Notes Archive	www.samba.org text/html	CONFIRM www.samba.org/samba/history/samba-4.0.11.html
openSUSE-SU-2013:1921-1: moderate: update for samba	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1921

openSUSE-SU-2013:1742-1: moderate: samba: security and bugfix update	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1742

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	4.0.2	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	4.0.0	All	All	All
Application	Samba	Samba	4.0.1	All	All	All
Application	Samba	Samba	4.0.10	All	All	All
Application	Samba	Samba	4.0.2	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

cpe:2.3:a:samba:samba:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:samba:samba:4.0.1:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.10:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.2:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.3:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.4:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.5:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.6:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.7:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.8:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.9:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.1.0:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.0:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.1:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.10:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.2:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.3:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.4:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.5:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.6:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.7:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.8:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.0.9:*:*:*:*:*:*:*

cpe:2.3:a:samba:samba:4.1.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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.

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