# Alpine Linux - Bug #9707

Bug # 9705 (Closed): samba: Multiple vulnerabilities (CVE-2018-14629, CVE-2018-16841, CVE-2018-16851)

## [3.8] samba: Multiple vulnerabilities (CVE-2018-14629, CVE-2018-16841, CVE-2018-16851)

11/28/2018 10:05 AM - Alicha CH

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 11/28/2018 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Natanael Copa | **% Done:** | 100% |
| **Category:** | Security | **Estimated time:** | 0.00 hour |
| **Target version:** | 3.8.2 | | |
| **Affected versions:** | | **Security IDs:** | CVE-2018-14629, CVE-2018-16841, CVE-2018-16851 |

**Description**

## CVE-2018-14629: Unprivileged adding of CNAME record causing loop in AD Internal DNS server

All versions of Samba from 4.0.0 onwards are vulnerable to infinite query recursion caused by CNAME loops. Any dns record can be added via ldap by an unprivileged user using the ldbadd tool, so this is a security issue.

### Fixed In Version:

Samba 4.7.12, 4.8.7, and 4.9.3

### References:

https://www.samba.org/samba/security/CVE-2018-14629.html
https://www.samba.org/samba/history/security.html

## CVE-2018-16841 : Double-free in Samba AD DC KDC with PKINIT

A flaw was found in Samba from 4.3.0 versions. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ.
This is only possible after authentication with a trusted certificate. This could result in a Denial of Service attack.

### Fixed In Version:

Samba 4.7.12, 4.8.7 and 4.9.3

### References:

https://www.samba.org/samba/security/CVE-2018-16841.html
https://www.samba.org/samba/history/security.html

## CVE-2018-16851: NULL pointer de-reference in Samba AD DC LDAP server

A flaw was found in Samba versions from 4.0.0. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. This can lead to a denial of service attack.

### Fixed In Version:

Samba 4.7.12, 4.8.7 and 4.9.3

### References:

https://www.samba.org/samba/security/CVE-2018-16851.html
https://www.samba.org/samba/history/security.html

### History

**#1 - 12/18/2018 05:01 PM - Natanael Copa**

*- Status changed from New to Resolved*

*- % Done changed from 0 to 100*

fixed with alpine:bd73fabb2c22b54983d0f10ae0d7c7b441b26001

**#2 - 02/19/2019 11:51 AM - Alicha CH**

*- Project changed from Alpine Security to Alpine Linux*

*- Category set to Security*

*- Status changed from Resolved to Closed*