FreeNAS - Bug #59994

Fix multiple CVEs affecting Samba 4.9 port

11/27/2018 06:10 AM - Dru Lavigne

Status:	Done		
Priority:	No priority		
Assignee:	Andrew Walker		
Category:	Services		
Target version:	Master - FreeNAS Nightlies		
Seen in:		**Needs Merging:**	No
Severity:	New	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	No	**ChangeLog Required:**	No
Needs Doc:	No		

Description

```
Release Announcements
---------------------

These are security releases in order to address the following defects:

o  CVE-2018-14629 (Unprivileged adding of CNAME record causing loop in AD
                   Internal DNS server)
o  CVE-2018-16841 (Double-free in Samba AD DC KDC with PKINIT)
o  CVE-2018-16851 (NULL pointer de-reference in Samba AD DC LDAP server)
o  CVE-2018-16852 (NULL pointer de-reference in Samba AD DC DNS servers)
o  CVE-2018-16853 (Samba AD DC S4U2Self crash in experimental MIT Kerberos
                   configuration (unsupported))
o  CVE-2018-16857 (Bad password count in AD DC not always effective)

CVE-2018-16852 and CVE-2018-16857 affect 4.9 only.

=======
Details
=======

o  CVE-2018-14629:
   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.

o  CVE-2018-16841:
   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.

   talloc is robust against further corruption from a double-free with
   talloc_free() and directly calls abort(), terminating the KDC process.

   There is no further vulnerability associated with this issue, merely a
   denial of service.

o  CVE-2018-16851:
```

```
   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.

   There is no further vulnerability associated with this issue, merely a
   denial of service.

o  CVE-2018-16852:
   During the processing of an DNS zone in the DNS management DCE/RPC server,
   the internal DNS server or the Samba DLZ plugin for BIND9, if the
   DSPROPERTY_ZONE_MASTER_SERVERS property or DSPROPERTY_ZONE_SCAVENGING_SERVERS
   property is set, the server will follow a NULL pointer and terminate.

   There is no further vulnerability associated with this issue, merely a
   denial of service.

o  CVE-2018-16853:
   A user in a Samba AD domain can crash the KDC when Samba is built in the
   non-default MIT Kerberos configuration.

   With this advisory we clarify that the MIT Kerberos build of the Samba
   AD DC is considered experimental.  Therefore the Samba Team will not
   issue security patches for this configuration.

o  CVE-2018-16857:
   AD DC Configurations watching for bad passwords (to restrict brute forcing
   of passwords) in a window of more than 3 minutes may not watch for bad
   passwords at all.

For more details and workarounds, please refer to the security advisories.
```

Related issues:

Copied from FreeNAS - Bug #59985: Fix multiple samba CVEs	**Done**

History

#1 - 11/27/2018 06:10 AM - Dru Lavigne

- Copied from Bug #59985: Fix multiple samba CVEs added

#2 - 11/27/2018 06:11 AM - Dru Lavigne

Samba 4.9 - freenas/ports
Master PR - https://github.com/freenas/ports/pull/172

#3 - 11/27/2018 06:14 AM - Dru Lavigne

- Subject changed from Fix multiple samba CVEs to Fix multiple CVEs affecting Samba 4.9 port

#5 - 01/04/2019 11:32 AM - Andrew Walker

- Status changed from In Progress to Closed

- Needs QA changed from Yes to No

- Needs Doc changed from Yes to No

- Needs Merging changed from Yes to No

#6 - 01/21/2019 11:02 AM - Dru Lavigne

- Target version changed from 11.3 to 11.3-BETA1

#7 - 01/23/2019 10:39 AM - Dru Lavigne

- Status changed from Closed to Done

- Target version changed from 11.3-BETA1 to Master - FreeNAS Nightlies