Alpine Linux - Bug #9803

Bug # 9801 (Closed): krb5: Ignore password attributes for S4U2Self requests (CVE-2018-20217)

[3.8] krb5: Ignore password attributes for S4U2Self requests (CVE-2018-20217)

12/27/2018 08:44 AM - Alicha CH

Status:	Closed	**Start date:**	12/27/2018
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-2018-20217

Description

A Reachable Assertion issue was discovered in the KDC in MIT Kerberos 5 (aka krb5) before 1.17. If an attacker can obtain a krbtgt ticket using
an older encryption type (single-DES, triple-DES, or RC4), the attacker can crash the KDC by making an S4U2Self request.

References:

https://nvd.nist.gov/vuln/detail/CVE-2018-20217
http://krbdev.mit.edu/rt/Ticket/Display.html?id=8763

Patch:

https://github.com/krb5/krb5/commit/5e6d1796106df8ba6bc1973ee0917c170d929086

Associated revisions

Revision 7972b2ef - 01/07/2019 07:57 AM - Leonardo Arena

main/krb5: upgrade to 1.15.4, security fix for CVE-2018-20217

Fixes #9803

History

#1 - 01/07/2019 07:57 AM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:7972b2ef858d1a229aac295737e382b6a30af0ca.

#2 - 01/09/2019 07:15 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed