Installer - Feature #21756

Update bind puppet module to use FIPS-approved hash function for dhcpd shared secret

11/23/2017 08:53 PM - Anonymous

Status:	Rejected		
Priority:	Normal		
Assignee:			
Category:	Foreman modules		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/puppet-dns/pull/103		

Description

Related issues:

Related to Foreman - Feature #3511: As a security person, I would like Forem...	**Resolved**

History

#1 - 11/23/2017 08:54 PM - Anonymous

- Related to Feature #3511: As a security person, I would like Foreman to run in FIPS mode added

#2 - 11/23/2017 09:59 PM - Ewoud Kohl van Wijngaarden

- Status changed from New to Need more information

I'd argue this is currently a CANTFIX. According to rdnc.conf (https://linux.die.net/man/5/rndc.conf):

> The key statement begins with an identifying string, the name of the key. The statement has two clauses. algorithm identifies the encryption algorithm for rndc to use; **currently only HMAC-MD5 is supported**. This is followed by a secret clause which contains the base-64 encoding of the algorithm's encryption key. The base-64 string is enclosed in double quotes.

#3 - 11/23/2017 10:11 PM - Ewoud Kohl van Wijngaarden

Oh, looks like you can also use dnssec-keygen rather than rndc-confgen so maybe it's possible.

#4 - 11/24/2017 10:10 PM - The Foreman Bot

- Status changed from Need more information to Ready For Testing

- Assignee set to Anonymous

- Pull request https://github.com/theforeman/puppet-dns/pull/103 added

#5 - 11/24/2017 10:43 PM - Anonymous

Hash functions other than MD5 are supported in bind (and rndc-config) versions 9.10.0 and higher. See https://source.isc.org/cgi-bin/gitweb.cgi?p=bind9.git;a=commit;h=4eb998928b9aef0ceda42d7529980d6581138698a for details.

#6 - 11/27/2017 09:30 PM - Anonymous

Both bind and dhcpd use isc's implementations of crypto hash functions (including MD5) and appear to be unaffected by openssl operating in FIPS mode. I don't think any actions are required.

#7 - 12/15/2017 09:43 PM - Anonymous

- Status changed from Ready For Testing to Resolved

#8 - 12/15/2017 11:15 PM - Ewoud Kohl van Wijngaarden

- Status changed from Resolved to Rejected