CipherShed - Bug #28

Audit of 04af5c7 - Buffer Overflow: strcat

12/19/2014 05:45 AM - Jason Pyeron

Status:	Resolved	**Start date:**	12/19/2014
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.7.3 Alpha	**Spent time:**	0.00 hour

Description

4.2. Buffer Overflow: strcat

4.2.1. File ~~1~~.2.43
4.2.1.1. The code in this file executes with elevate permissions.
4.2.1.2. In several locations a path is checked for a trailing backslash (0x5c), and if none is found one is appended. The appending operation never checks if the destination has sufficient allocated memory for one more char.
4.2.1.3. Other places the function is used to append arbitrary string constants to a string on the heap, e.g. 'strcat (path, "\\TrueCrypt")'.
4.2.1.4. If the application does not crash from the execution of the strcat, the modified memory is then passed into system calls, e.g. '_stat (path, &st)'.

History

#1 - 12/19/2014 10:35 PM - Jason Pyeron

- Status changed from New to Resolved

[v0.7.3.0-dev 8bb2cc0] resolves https://issues.ciphershed.org/issues/28
1 file changed, 18 insertions(+), 18 deletions(-)

jpyeron@black /projects/cipherShed
$ git log -1
commit 8bb2cc05d1e1c808bc6c8aee63e678034fe9f31e
Author: Jason Pyeron <jpyeron@pdinc.us>
Date: Fri Dec 19 09:36:24 2014 -0500

```
resolves https://issues.ciphershed.org/issues/28


fixed other strcat calls as found
```

#2 - 12/21/2014 08:57 PM - Rocki H

- Target version set to 0.7.3 Alpha