CipherShed - Bug #27

Audit of 04af5c7 - Buffer Overflow: sprintf

12/19/2014 05:43 AM - Jason Pyeron

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

Description

4.1. Buffer Overflow: sprintf

4.1.1. File ~~1~~.2.43
4.1.1.1. The code in this file executes with elevate permissions.
4.1.1.2. The DoTrueCryptShortcutsUninstall function uses szTmp2 string to hold computed paths. The input to sprintf are strings which can be longer than the destination, e.g. 'sprintf (szTmp2, "%s%s", szLinkDir, "\\TrueCrypt.lnk")'.
4.1.1.3. If the application does not crash from the execution of the sprintf, the modified memory is then passed into system calls, e.g. 'StatDeleteFile (szTmp2)'.

History

#1 - 12/19/2014 10:24 PM - Jason Pyeron

- Status changed from New to Resolved

[pyeron-issues.ciphershed.org-27 b42e525] resolves https://issues.ciphershed.org/issues/27
2 files changed, 36 insertions(+), 34 deletions(-)

jpyeron@black /projects/cipherShed
$ git log -1
commit b42e5256fe6dcd0deb16a5b534922c73c5791e41
Author: Jason Pyeron <jpyeron@pdinc.us>
Date: Fri Dec 19 09:25:19 2014 -0500

```
resolves https://issues.ciphershed.org/issues/27


fix other sprintf calls found along the way. There are still many more calls to sprintf and wsprintf in the so
urce as a whole.
```

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

- Target version set to 0.7.3 Alpha