CipherShed - Bug #84

wcsncpy is subject to buffer overflow

01/18/2015 09:54 PM - Jason Pyeron

Status:	New	**Start date:**	01/18/2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

from http://www.cplusplus.com/reference/cwchar/wcsncpy/ :
"No null wide character is implicitly appended at the end of destination if source is longer than num (thus, in this case, destination may not be a null terminated C wide string)."

use wcsncpy_s http://msdn.microsoft.com/en-us/library/5dae5d43.aspx

on 54d5fe54ccbdca2e490d8f4f3bc5076eaada4497 grep says -

Common/Dlgcode.c:1136:
Common/Dlgcode.c:1142:
Common/Dlgcode.c:1187:
Common/Dlgcode.c:1201:
Common/Dlgcode.c:1226:
Common/Dlgcode.c:7663:
Common/Dlgcode.c:7664:
Driver/Ntvol.c:655:
Format/Tcformat.c:3772:
Format/Tcformat.c:3776:
Format/Tcformat.c:3921:
Format/Tcformat.c:3931:
Mount/Hotkeys.c:115:
Setup/Wizard.c:571: