



Riccardo Agostino
Monti

S7 L4

BUFFER OVERFLOW

Scopo del test

Modificare uno script in modo da risolvere il problema dell'overflow.

afeSEH	ASLR	NXCompat	OS DLL	Version	Path
True	False	False	True	5.1.2600	11 (C:\WINDOWS\Files\Audio.dll)
True	False	False	False	-1.0- [SDB]	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	6.00.2900.	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	8.00.6001.18702	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	False	False	False	1.2.12.0 [SDL]	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [DHC]	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.131.2600.5512 [DHC]	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [xpsp2]	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	False	1.0.0.402 [SysInfo.dll]	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	7.0.2600.5512 [msvcrtd.dll]	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	False	0.8.22.5506 [AudioCoder.exe]	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [RPCRT4.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [ntdll.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	False	-1.0- [libxml2.dll] (C:\Program Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [wshtopip.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	8.00.6001.18702 [ieframe.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [sensapi.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [RASAPI32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	8.00.6001.18702 [iertutil.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [IMAGEHELP.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [rasadhlp.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [Secur32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [WSOCK32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	6.00.2900.5512 [shdocvw.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [WS2HELP.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [ole32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [IMM32.DLL] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [thnetcfg.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [USER32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	False	False	False	1.18 [libiconv-2.dll] (C:\Program Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.131.2600.5512 [CRYPTUI.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [rtutil.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [IPHLPAPI.DLL] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.131.2600.5512 [WINTRUST.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	2001.12.4414.700 [COMRes.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [OLEAUT32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [rasman.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	6.00.2900.5512 [SHELL32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	True	False	False	-1.0- [mcores.dll] (C:\Program Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [DNSAPI.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	2001.12.4414.700 [CLBCATQ.DLL] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	6.0 [comct132.dll] (C:\WINDOWS\WinSxS\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [MSACM32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	False	1.1.0.0 [dsp_chmx.dll] (C:\Program Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	8.00.6001.18702 [WININET.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	6.00.2900.5512 [SHLWAPI.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [AVIFIL32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [msctfimeime] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [MSCTF.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	False	-1.0- [dsp_zsc.dll] (C:\Program Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.82 [COMCTL32.dll] (C:\WINDOWS\system\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [USERENV.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [WINMM.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [kernel32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [GDI32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	False	-1.0- [mccommon.dll] (C:\Program Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	6.00.2900.5512 [uxtheme.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	False	-1.0- [jpeg.dll] (C:\Program Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [WLDAP32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [msv1_0.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [VERSION.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [ADVAPI32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [PSAPI.DLL] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [WS2_32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	5.1.2600.5512 [mswsock.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
True	False	False	True	6.0.5441.0 [Normaliz.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)
False	True	False	True	5.1.2600.5512 [TAPI32.dll] (C:\WINDOWS\Files\Audiodrv.dll)	11 (C:\WINDOWS\Files\Audiodrv.dll)

Codice Modificato:

```
#include <stdio.h>
int main() {
    char buffer[30];
    printf ("Si prega di inserire il nome utente:");
    scanf ("%s", buffer);
    printf ("Nome utente inserito: %s\n", buffer);
    return 0;
```

Test del Codice

```
(kali㉿kali) - [ ~/Desktop ]
$ ./BOF
Si prega di inserire il nome utente:8739102733717093271990172381
Nome utente inserito: 8739102733717093271990172381
```