

[NT] WinRAR Filename Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00018.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 4 Jan 2006 17:38:11 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

WinRAR Filename Buffer Overflow

SUMMARY

" <<http://www.rarlab.com/>> WinRAR is a powerful archive manager."

By giving non ASCII characters to a filename compressed by WinRAR, attackers can execute arbitrary code by overflowing WinRAR internal buffer overflows.

DETAILS

Vulnerable Systems:

- * WinRAR English version 3.51

When using the "Add to archive" command in right click menu to create a compressed file on Windows Explorer, if there are some non-default-codepage and non-ASCII characters in the name of the file(s) to be compressed, a buffer overflow will occurred.

```
0048CFAE mov edx,dword ptr ds:[4a330c]
0048CFB4 mov eax, edx
0048D028 mov ecx, [eax] ; [1]
0048D08B mov [edx+ecx], ebx
```

[NT] WinRAR Filename Buffer Overflow

004A330C 2C AF A0 00

00A0AEEC 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64
00A0AEFC 20 53 65 74 74 69 6E 67 73 5C 41 64 6D 69 6E 69
00A0AF0C 73 74 72 61 74 6F 72 5C B9 D9 C5 C1 20 C8 AD B8
00A0AF1C E9 5C 3F E9 A9 3F 3F 3F D9 A5 3F 3F 3F 3F DB F5
00A0AF2C 2E 64 6F 63

0040ACC4 mov ecx, 10000000h ; cbMultiByte
0040ACC9 mov edx, [ebp+lpMultiByteStr] ; lpMultiByteStr
0040ACCF mov eax, esi ; lpWideCharStr
0040ACD1 call sub_40F874

0040F874 push ebx
0040F875 push esi
0040F876 mov esi,ecx
0040F878 mov bl,1
0040F87A push 0 ; /pDefaultCharUsed = NULL
0040F87C push 0 ; |pDefaultChar = NULL
0040F87E push esi ; |MultiByteCount = 10000000h
0040F87F push edx ; |MultiByteStr = [2]
0040F880 push -1 ; |WideCharCount = FFFFFFFFh
0040F882 push eax ; |WideCharStr
0040F883 push 0 ; |Options = 0
0040F885 push 0 ; |CodePage = CP_ACP
0040F887 call WideCharToMultiByte ; \WideCharToMultiByte

[1]: %eax should be sum of filename-base and strlen, but %eax will be incorrect in the environment mention above.

[2]: The WideCharToMultiByte API will overwrite the pointer referenced by

[1]

ADDITIONAL INFORMATION

The information has been provided by <<mailto:agoanywhere@xxxxxxxxxxxxx>>
agoanywhere.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

[NT] WinRAR Filename Buffer Overflow

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [*\[TOOL\] Arudius – Information Security Oriented Live CD Linux Distribution*](#)
 - Next by Date: [*\[TOOL\] Unhide – a Forensic Tool to Uncover Hidden Processes*](#)
 - Previous by thread: [*\[TOOL\] Arudius – Information Security Oriented Live CD Linux Distribution*](#)
 - Next by thread: [*\[TOOL\] Unhide – a Forensic Tool to Uncover Hidden Processes*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)