

[NT] PGP with Outlook Stores Password Pass Phrases in the Clear

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0129.html>

From: support@securiteam.com

Date: 03/31/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 31 Mar 2002 15:33:50 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

PGP with Outlook Stores Password Pass Phrases in the Clear

SUMMARY

Outlook can be integrated to use PGP. The integration allows users to almost seamlessly encrypt and decrypt emails, sign content, and use PGP's features without the hassle of a 3rd-party front-end. A security vulnerability has been found that would allow a local attacker to gain access to the pass phrase used by the user by analyzing the memory core dump caused by the crashing Outlook client.

DETAILS

Vulnerable systems:

PGP version 7.x and older

By default everyone can read at least, drwtsn32.log located in:

Under Windows 2000, it is located at:

C:\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log

Under Windows NT, it is located at:

C:\Winnt\System32\drwtsn32.log

Securiteam: [NT] PGP with Outlook Stores Password Pass Phrases in the Clear

Whenever the Outlook (with PGP integrated into it) client crashes it will core dump its memory content into a file (drwtsn32.log), this file has been found to contain the password used by the encrypting user in plain text.

Example drwtsn32.log:

```
function: TranslateMessageEx
77e1323a 0f8500c40200 jne EnumDesktopWindows+0xd88 (77e3f640)
77e13240 33c0 xor eax,eax
77e13242 c20800 ret 0x8
77e13245 ff742408 push dword ptr [esp+0x8] ss:043bd52b=?
77e13249 51 push ecx
77e1324a e8b7370000 call GetKeyState+0x92 (77e16a06)
77e1324f ebf1 jmp DialogBoxIndirectParamAorW+0x6ba
(77e1eb42)
77e13251 b89a110000 mov eax,0x119a
77e13256 8d542404 lea edx,[esp+0x4] ss:043bd52b=?
77e1325a cd2e int 2e
77e1325c c21000 ret 0x10
```

-----> Stack Back Trace <-----

```
FramePtr ReturnAd Param#1 Param#2 Param#3 Param#4 Function Name
0370FF78 77575C36 0370FF98 00000000 00000000 00000000
user32!TranslateMessageEx
0370FFB4 77E8758A 0000047C 77595428 0006F204 0000047C
winmm!midiOutGetNumDevs
0370FFEC 00000000 77575BB9 0000047C 00000000 037100A0
kernel32!SetFilePointer
```

-----> Raw Stack Dump <-----

```
0370ff58 63 58 e1 77 98 ff 70 03 - 00 00 00 00 00 00 00 00
cX.w..p.....
0370ff68 00 00 00 00 7c 04 00 00 - 00 00 00 00 27 58 e1 77
...|.....'X.w
0370ff78 b4 ff 70 03 36 5c 57 77 - 98 ff 70 03 00 00 00 00
.p.6\Ww..p....
0370ff88 00 00 00 00 00 00 00 00 - 28 54 59 77 04 f2 06 00
.....(TYw....
0370ff98 20 20 32 81 ff ff ff ff - 77 0d 43 80 00 00 00 00 2.....w.C.....
0370ffa8 00 00 00 00 00 00 00 00 - 7b 10 43 80 ec ff 70 03
.....{.C...p.
0370ffb8 8a 75 e8 77 7c 04 00 00 - 28 54 59 77 04 f2 06 00
u.w|...(TYw....
0370ffc8 7c 04 00 00 00 f0 fa 7f - 00 00 57 77 c0 ff 70 03
|.....Ww..p.
0370ffd8 00 00 57 77 ff ff ff ff - 5b 61 e8 77 80 b5 e8 77
.Ww....[a.w...w
0370ffe8 00 00 00 00 00 00 00 00 - 00 00 00 00 b9 5b 57 77
.....[Ww
0370fff8 7c 04 00 00 00 00 00 00 - a0 00 71 03 00 00 00 00
```

Securiteam: [NT] PGP with Outlook Stores Password Pass Phrases in the Clear

```

|.....q.....
03710008 03 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00
.....
03710018 00 00 00 00 00 00 00 00 – a0 00 71 03 00 00 71 03
.....q...q.
03710028 02 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00
.....
03710038 00 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00
.....
03710048 00 00 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00
.....
03710058 00 00 00 00 00 00 00 00 – a0 07 e4 01 6b 00 00 00
.....k...
03710068 46 47 55 42 00 00 00 00 –
PASSPHRASEVALUEISHEREPAFGUB...PASSPHRA
03710078 PASSPHRASEVALUEISHEREPA –
PASSPHRASEVALUEISHEREPAASEVALUESISHEREP
03710088 7d 40 00 00 00 00 00 00 – 00 00 00 00 00 00 00 00
AS.....

```

ADDITIONAL INFORMATION

The information has been provided by NtWaK0.

=====

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@securiteam.com
 In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.



- **Previous message:** support@securiteam.com: "[TOOL] WhiteHat Arsenal (Web Based Security Audit)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)