

[NT] Novell GroupWise Client Integer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0113.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/29/05

To: list@securiteam.com

Date: 29 Sep 2005 15:13:15 +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>

Novell GroupWise Client Integer Overflow

SUMMARY

" <<http://www.novell.com/products/groupwise/index.html>> Novell GroupWise is a complete collaboration software solution that provides information workers with e-mail, calendaring, instant messaging, task management, and contact and document management functions."

Novell GroupWise Client is vulnerable to a integer overflow that allows attackers to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * GroupWise version 6.5.3

Immune Systems:

- * GroupWise version 6.5 SP5

The integer overflow bug is due to failure of the application to parse the saved port number stored in Windows' registry.

Proof of Concept:

To reproduce this, we have to modify the default register key of

Securiteam: [NT] Novell GroupWise Client Integer Overflow

HKEY_CURRENT_USER\Software\Novell\GroupWise\Login Parameters\TCP/IP Port

For example, set the value (11111111111111111111111111111111).

Then, when we open the application client and the client get the port information occur the integer overflow.

Stack Trace:

```
EAX C71C71C7
ECX 01F6ADC0 ASCII "10.1.1.1"
EDX 01F6ADC0 ASCII "10.1.1.1"
EBX 00000000
ESP 0012E9DC
EBP 0012E9EC
ESI 00000000
EDI 00000000
EIP 52080AB3 gwenv1.52080AB3
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 1 FS 0038 32bit 7FFDE000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010292 (NO,NB,NE,A,S,PO,L,LE)
ST0 empty -NAN FFFF FFFCFEFC FFFCFEFC
ST1 empty -??? FFFF 00000000 00000000
ST2 empty -??? FFFF 00FE00FB 00FD00FB
ST3 empty -??? FFFF 00FE00FB 00FD00FB
ST4 empty -NAN FFFF FFFCFEFC FFFCFEFC
ST5 empty -??? FFFF 00FF00FC 00FE00FC
ST6 empty -??? FFFF 00000000 00000000
ST7 empty 256.000000000000000000
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
```

Assembly code:

```
52080AB3 66:8B00 MOV AX,WORD PTR DS:[EAX]
```

Vendor Status:

The vendor has issued a patch:

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2972191.htm>
<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2972191.htm>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2804>
CAN-2005-2804

Securiteam: [NT] Novell GroupWise Client Integer Overflow

Disclosure Timeline:

- 07/28/2005 – Initial vendor notification
- 07/28/2005 – Initial vendor response notify research
- 08/07/2005 – Second vendor response
- 09/27/2005 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:famato@infobyte.com.ar>
Francisco Amato.

<<http://support.novell.com/techcenter/search/search.do?cmd=displayKC&docType=kc&externalId=10098814html&sl>>

The vendor advisory

=====

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.