

# [NT] Novell GroupWise Client Buffer Overflow

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0009.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 08/01/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 1 Aug 2005 19:06:13 +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 Buffer Overflow

---

## SUMMARY

" <<http://www.novell.com>> GroupWise Client is Novell's premier Intranet/Internet GroupWare solution for platform Windows."

Lack of proper text phrasing of a text file allows attackers to exploit a buffer overflow vulnerability in Novell GroupWise Windows Application and execute arbitrary code.

## DETAILS

Vulnerable Systems:

- \* GroupWise version 6.5.3

Immune Systems:

- \* GroupWise version 6.5 SP5

A buffer overflow vulnerability by phrasing a specially crafted GWVW02???.INI file allow attackers to execute arbitrary code on the system.

In order to take advantage of this vulnerability, attackers needs to gain access to the post office directory. On a well configured servers, access to this folder is typically limited to the system administrator.

## Securiteam: [NT] Novell GroupWise Client Buffer Overflow

In order to create a crafted GWVW02???.INI file, it is possible to take sections such as [Group Task] and set a label of ES02TKS.VEW with the value ("A" x 174).

Then, when users open the client application and perform the authentication, the buffer overflow was already made.

### Information of Registers:

```
EAX 00000001
ECX 7FFDE000
EDX 00E80608
EBX 41414141
ESP 0012F74C
EBP 0012F7B0
ESI 00E80000
EDI 41414139
EIP 78495BA9 ntdll.78495BA9
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 0038 32bit 7FFDE000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty - NAN FFFF FFF8FCF8 FFF8FCF8
ST1 empty - ??? FFFF 00000000 00000000
ST2 empty - ??? FFFF 00FE00F7 00FB00F7
ST3 empty - ??? FFFF 00FE00F7 00FB00F7
ST4 empty - NAN FFFF FFF8FCF8 FFF8FCF8
ST5 empty - ??? FFFF 00FF00F8 00FC00F8
ST6 empty - ??? FFFF 00000000 00000000
ST7 empty 256.00000000000000000000
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 line:

```
78495BA9 0FB707 MOVZX EAX,WORD PTR DS:[EDI]
```

If attackers have access to the post offices and place the GWVW02???.INI file, they could have the possibility of compromise every user that use the Novell GroupWise Windows Application.

### Vendor Status:

The vendor has released a patch:

<<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2971927.htm>>  
<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2971927.htm>

### Disclosure Timeline:

07/05/2005 - Initial vendor notification

Securiteam: [NT] Novell GroupWise Client Buffer Overflow

07/06/2005 – Initial vendor response  
07/27/2005 – Coordinated public disclosure

ADDITIONAL INFORMATION

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

The original article can be found at:  
<<http://www.infobyte.com.ar/adv/ISR-12.html>>  
<http://www.infobyte.com.ar/adv/ISR-12.html>

The Vendor advisory can be found at:  
<<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098314.htm>>  
<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098314.htm>

=====

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.