

BakBone NetVault Remote Heap Buffer Overflow

discovered and expl0ited by class101

www.class101.org

www.hat-squad.com

-
- I. Advisory url
 - II. Application overview
 - III. Vulnerability
 - IV. Poc exploit
 - V. Patch
 - VI. Disclosure timeline

I. ADVISORY URL

- <http://www.hat-squad.com/en/000164.html>
- <http://www.class101.org/netv-remhbof.pdf>

II. APPLICATION OVERVIEW

NetVault™ is a professional backup and restore solution for individual Windows and Linux servers and very small heterogeneous UNIX, Windows NT/2000, Linux and Netware environments. A modular architecture allows NetVault™ to combine with BakBone's plugin modules for enhanced features such as application data protection, disaster recovery, NDMP and open file protection.

BakBone Software's® NetVault 7 delivers enhanced data protection and enterprise-class functionality that scales to meet the demands of any sized environment. With the release of NetVault 7, users will benefit from increased automation, enhanced administrator productivity, and rapid deployment.

Enhanced platform support

- Microsoft Cluster Server (MSCS)
- Windows 2000
- Windows 2003/XP
- Red Hat Enterprise Linux RHCS
- Linux Kernel 2.4
- Linux Kernel 2.6

NetVault 7.3 Application Support (for applications running in a cluster)

- MS-SQL 7.0
- MS-SQL 2000
- MS Exchange 2000
- MS Exchange 2003

BakBone NetVault Remote Heap Buffer Overflow

discovered and expl0ited by class101

www.class101.org

www.hat-squad.com

-
- I. Advisory url
 - II. Application overview
 - III. Vulnerability
 - IV. Poc exploit
 - V. Patch
 - VI. Disclosure timeline

III. VULNERABILITY

Heap: Area of memory that a program uses to store large buffers such client/server requests

While having a look at the communication protocol used by the netvault's client/server, the hat-squad has discovered several obscure points, as the possibility to guess the computername, to notice several bytes in the buffer referring to a string size stored in the heap :P.. While playing with such datas, a malicious user can add his own server entry to the "Available NetVault Machines" list nor at best for him, to override the heap where is stored the submitted "clientname" and to finally control two pointers in the heap management structure. Once freed or allocated; the heap is moving one pointer into the second and the second into the first.

```
77F37111 8901 MOV DWORD PTR DS:[ECX],EAX
77F37113 8948 04 MOV DWORD PTR DS:[EAX+4],ECX
```

Needless to say that owning both pointers, the attacker is able to overwrite any windows function marked as writable with any 32 bits value we want. To HeapAllocate at around 33000 bytes will produce an access violation.

I expect several hours of work from NetVault Tech Team to fix all their unsecured codes because assuming that we found 2 holes in 2 days in a so professional product, let us to think that the whole backup software is unsecured and so on, and so forth :(

IV. POC EXPLOIT

The public poc has been tested successfully on:

- Windows 2000 SP4 Server EN
- Windows 2000 SP4 Advanced Server EN
- Windows 2000 SP4 Professional EN
- Windows XP SP1a Professional EN
- Windows XP SP1 Professional EN

Exploitation methods:

- UnhandledExceptionFilter (uncommented)
- RtlEnterCriticalSection (commented)

BakBone NetVault Remote Heap Buffer Overflow

discovered and expl0ited by class101

www.class101.org

www.hat-squad.com

-
- I. Advisory url
 - II. Application overview
 - III. Vulnerability
 - IV. Poc exploit
 - V. Patch
 - VI. Disclosure timeline
-

Unpublished code:

- Windows 2003 SP0 Server EN
- Windows XP SP2 Professional EN

The public poc can be downloaded at hat-squad.com and class101.org and proly all security websites. If I had to rate the stability of it, this is 90% rate success, the other 10% will give you sometimes the shell after that the attacker establish a second connection to the server or an access violation replacing our "where" pointer by another one pointing to our buffer. This might still be exploited but the attacker has to guess if his hacking attempt will fail or succeed the first time. On SP2 and Windows 2003, this is not possible to exploit via this way because of a security check added to ntdll.dll

```
77F370FE 8B39          MOV EDI,DWORD PTR DS:[ECX]
77F37100 3B78 04       CMP EDI,DWORD PTR DS:[EAX+4]
77F37103 0F85 F4FCFFFF JNZ ntdll.77F36DFD          if [ECX] == [EAX+4] goto Heap.corruption
77F37109 3BFA          CMP EDI,EDX
77F3710B 0F85 ECFCFFFF JNZ ntdll.77F36DFD          if [ECX] == EDX goto Heap.corruption
77F37111 8901          MOV DWORD PTR DS:[ECX],EAX
77F37113 8948 04       MOV DWORD PTR DS:[EAX+4],ECX
```

Due to the number of hours of work on it to passe 2k3 and SP2 and also regarding the high number of affected servers in big companies running Windows 2003 with NetVault, "remembering 2k3 + backupexec", thos targets wont remain in the public code.

V. PATCH

All 7.x versions have been tested vulnerable, the same results are to expect on 6.x serie.

At the moment writing this advisory, no patch were released, we can only suggest to restrict all incoming connections to 20031/tcp and 20031/udp, a fix might come very soon.

This is important to mention that we warned them several times via mails, phone calls, what do we got from their office is a: "when a man such you reports a security hole, we can not put all works on the ground and say yes: we are fixing it"

At least we know that Mr Doug Spencer, vice president of research and development bakbone software, will do something to fix this bug, recalling that we found bugs in smaller applications, fixed faster

Overflowed security response ?

BakBone NetVault Remote Heap Buffer Overflow

discovered and expl0ited by class101

www.class101.org

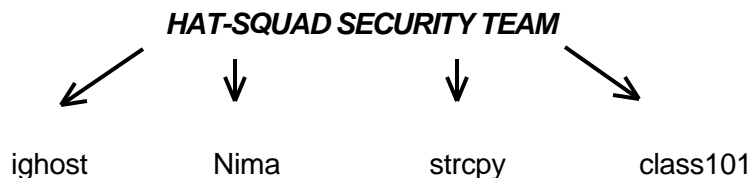
www.hat-squad.com

-
- I. Advisory url
 - II. Application overview
 - III. Vulnerability
 - IV. Poc exploit
 - V. Patch
 - VI. Disclosure timeline

VI. DISCLOSURE TIMELINE

16-3-2005: local stack BOF found
17-3-2005: vendor notification #1/3
18-3-2005: vendor notification #2/3
19-3-2005: vendor notification #3/3
19-3-2005: remote heap BOF found
21-3-2005: vendor RE-notification #1/1
24-3-2005: vendor wake up

GREETINGS



THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

Pejman/deject gone with the russians ?? whahahhahahahHAHAHAHAH, I dunno you but at least , we all know you are a stupid l00ser :->