

BakBone NetVault Local Stack 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/000165.html>
- <http://www.class101.org/netv-locsbof.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 Local Stack 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

The flaw reside in the "configure.cfg" file, configuring a computername "Name=" longer than 111 bytes will create an access violation at the next service restart. However, the risk is low on NTFS systems with Users:R by default.

A malicious user might still be able to run an arbitrary code with SYSTEM privilege once the "NetVault Process Manager" service will restart.

IV. POC EXPLOIT

The public poc has been tested successfully on:

-All Windows

Exploitation method:

-ExceptionHandlerPointer

BakBone NetVault Local Stack 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
-

The code overwrite the pointer to the exception handler by a jump from a netvault dynamic library.
Once the service will restart, the pointer will be changed to reach our shellcode adding a windows user: class101
pass: class101

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 set STRICTS ACL rules, for example, allow ONLY SYSTEM to write in configure.cfg. (nor to move from FAT to NTFS :p)

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 Local Stack Buffer Overflow

discovered and exploited 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

HAT-SQUAD SECURITY TEAM



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.