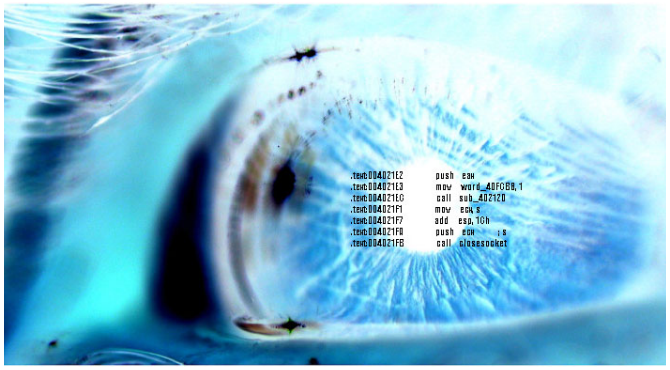
CIRT

Danish Computer Incident Response Team

Security advisory

Novell Nsure Audit 1.0.1 (Win32 version)



```
.text:004021E2          push  eax
.text:004021E3          mov   word_40FCB8,1
.text:004021EC          call  sub_402120
.text:004021F1          mov   ecx,s
.text:004021F7          add   esp,10h
.text:004021FA          push  ecx         ; s
.text:004021FB          call  closesocket
```

Discovered
by Dennis Rand
advisory@cirt.dk
http://www.cirt.dk

Table of contents

Table of contents 2
Introduction 3
Problem 3
Who are Novell 3
Timeline of public disclosure 4
Contact information 4
File description and MD5 checksum 5
MD5 software used 5
Novell Nsure Audit 1.0.1 5
Installation files: 5
Service file: 5
Technical details of the vulnerabilities 6
OpenSSL ASN.1 Parsing vulnerability 6
Corrective actions 7
Novell Nsure Audit 1.0.1 7
Disclaimer 7

Introduction

Problem

The installation has been made on a Windows 2000 server service pack 4 running with the latest patch level.

Novell Nsure Audit 1.0.1

- OpenSSL ASN.1 Parsing vulnerability

Who are Novell

Novell helps organizations determined to eliminate business obstacles and leverage their information assets by integrating their information, applications, processes and systems.
Novell delivers solutions including secure identity management, web services and application integration, and cross-platform networking services, all supported by strategic consulting, technical support and educational services.

http://www.novell.com/company/

Timeline of public disclosure

- 08-01-2005 Vulnerability discovered.
- 17-04-2005 Research ended.
- 18-04-2005 Novell Notified (secure@novell.com)
- 18-04-2005 Received response from Ed Reed, Security Tzar, Novell, Inc.
- 19-04-2005 Novell Fixes issue in Nsure Audit 1.0.1
- 24-04-2005 CIRT.DK Public release

Contact information

The following vulnerability were discovered by Dennis Rand at CIRT.DK
Questions regarding this issue should be directed to:

Dennis Rand
advisory@cirt.dk

File description and MD5 checksum

MD5 software used

Filename:	md5sum.exe
Comments:	Modified from the version originally developed by Ulrich Drepper <drepper@gnu.ai.mit.edu>
Company name:	GMG Systems, Inc.
Product name:	Forensic Acquisition Utilities
Product version:	1.0.0.1026
File version:	2.0.1.1032
MD5 checksum:	607be2b261c516a5c5469314445ab2f2

Novell Nsure Audit 1.0.1

Installation files:

Filename:	naudit_win32.exe
MD5 checksum:	7031b2c14e8f2bbf29b0b0d3efd68c6e

Service file:

Filename:	webadmin.exe (Novell Nsure Audit 1.0.1)
MD5 checksum:	b25a9ecb5855a016732379116afc134c
Description:	Novell® Nsure™ Audit Component
File version:	1.0.0.0
Product name:	Novell Nsure Audit
Product version:	1, 0, 0, 0
Novell Checksum:	2560 F7FC 5071 6066 7519 879A

Technical details of the vulnerabilities

OpenSSL ASN.1 Parsing vulnerability

Multiple vulnerabilities were reported in the ASN.1 parsing code in OpenSSL. These issues could be exploited to cause a denial of service or to execute arbitrary code.

When using the exploit downloaded from here:
http://www.securityfocus.com/data/vulnerabilities/exploits/ASN.1-Brute.c

The server will stop responding.

Output from attack:

```
[********************************** START *********************************************]
[root@localhost test]# ./a.out 192.168.1.4 449
OpenSSL ASN.1 brute forcer (Syzop/2003)

seed = 1135277150
.....................................................................................................................................................
.....................................................................................................................................................
.....................................................................................Unable to connect: Connection refused
DIFF:
Offset 71: 0xa -> 0xffffffe6
Offset 97: 0x6e -> 0x68
Offset 106: 0x6f -> 0xfffffff5
Offset 144: 0x32 -> 0xffffffcc
Offset 148: 0x30 -> 0x5b
Offset 154: 0x30 -> 0x2e
Offset 261: 0x6 -> 0x3a
Offset 563: 0x4e -> 0xffffffd1
Offset 583: 0x5c -> 0xffffffd8
Offset 629: 0xffffffa3 -> 0x67
Offset 718: 0xffffffa7 -> 0x41
Offset 719: 0xffffffa8 -> 0xffffffa5
Offset 770: 0x4d -> 0xffffffdf
Offset 773: 0xffffffae -> 0xffffffca
Offset 927: 0xffffff81 -> 0xffffffd5
*****
[********************************** STOP *********************************************]
```

At some points the exploit had to be run a few times, just stopped after 30 seconds and restarted

Vulnerable systems:

The webadmin.exe (Novell Nsure Audit 1.0.1) service running on port 449

Fix:

http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097379.htm

Corrective actions

Novell Nsure Audit 1.0.1

Document Title:	Security Vulnerability against webadmin.exe
Document ID:	10097379
Solution ID:	NOVL101807
Creation Date:	19APR2005
Modified Date:	19APR2005
Novell Product Class:	Connectivity Products

http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097379.htm

Disclaimer

The information within this document may change without notice.
Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall I be liable for any consequences or damages,
including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document
is the sole property of their respective owners.