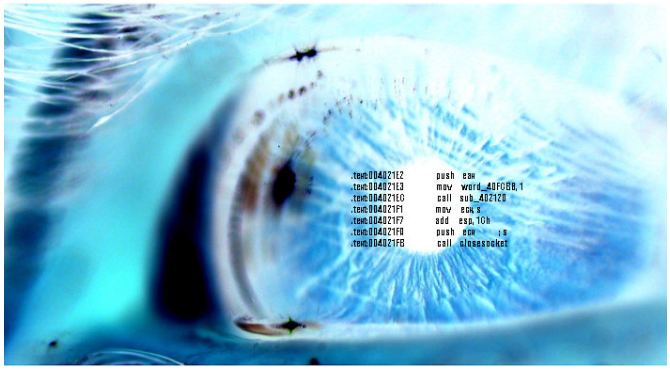
CIRT

Danish Computer Incident Response Team

Security advisory

Novell eDirectory 8.7.3 DOS Device name Denial of Service

CVE: CAN-2005-1729



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
    Novell information 3
Timeline of public disclosure 4
Contact information 4
File description and MD5 checksum 5
  MD5 software used 5
  Novell eDirectory 8.7.3 5
    Installation files: 5
    Service file: 5
Technical details of the vulnerabilities 6
    Requesting "DOS Device in Path Name" Denial of Service 6
Corrective actions 7
Disclaimer 7

Introduction

Problem

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

The Novell eDirectory 8.7.3

- Denial of Service requesting DOS Device in Path Name

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/

Novell information

ID:	NOVL102201
Domain:	primus
Solution Class:	Novell
Fact:	Novell eDirectory 8.7.3 for Windows 2000
Fact	Novell eDirectory 8.7.3 for Windows NT
Symptom:	Requesting "DOS Device in Path Name" Denial of Service
Symptom:	Attack causes error in dhost.exe application
Symptom:	Attack causes nds service to stop until manually restarted.
Symptom:	Problem is not reproducible when using the current interm release for eDirectory 8.7.3 which is currently IR6

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.
- 03-06-2005 Novell Fixes issue
- 13-06-2005 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 eDirectory 8.7.3

Installation files:

Filename:	NT65DE.exe
MD5 checksum:	7f945a7c5636b7b371a65d35dfac842d

Service file:

Filename:	dhost.exe
MD5 checksum:	32d1885ccba1f156bc56b40dd349632c
File version:	105.50.98.0
Product name:	Host Environment for Novell eDirectory
Product version:	8.7.3
Novell Checksum:	680B 7917 3EFF 9190 56F5 58D6

Technical details of the vulnerabilities

Requesting "DOS Device in Path Name" Denial of Service

The problem exhibits itself when requesting an URL that includes reserved MS-DOS devices. These represent devices such as the first printer port (LPT1) and the first serial communication port (COM1). Sample reserved MS-DOS device names include:

- AUX
- CON
- PRN
- COM1
- LPT1

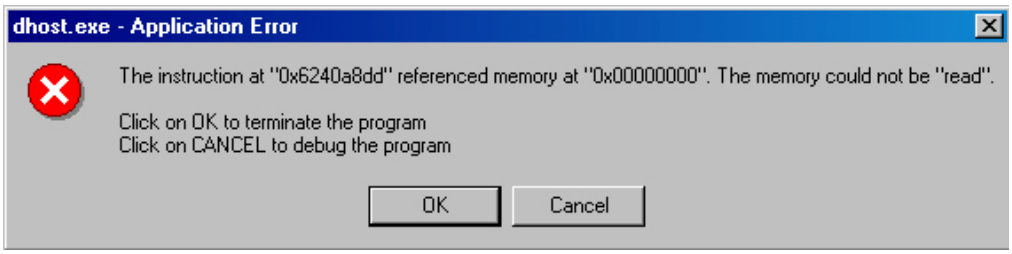
Default open web-ports:

- 8008 HTTP
- 8010 HTTPS

Proof-of-concept
http://target:8008/COM1
http://target:8008/COM2
http://target:8008/AUX

When the attack is preformed the service will stop, until manually restarted

The following error occurs, and are shown on the server



The vulnerable system is: **Novell eDirectory 8.7.3 Webserver**

Corrective actions

Fix: Apply the current interm release for eDirectory 8.7.3 available on the http://support.novell.com/novell

Disclaimer