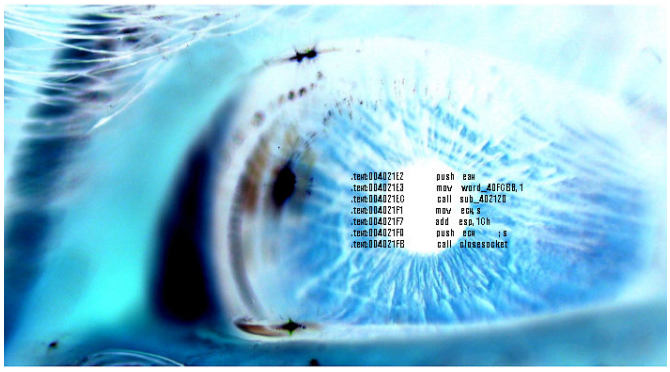
CIRT

Danish Computer Incident Response Team

Security advisory

Novell iManager 2.0.2 ASN.1 Parsing vulnerability in Apache module

CVE: CAN-2005-1730



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

Table of contents

Introduction

Problem

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

Novell iManager 2.0.2

- OpenSSL ASN.1 Parsing vulnerability in Apache module

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 Response

ID:	NOVL102200
Domain:	primus
Solution Class:	Novell
Fact:	Novell iManager 2.02
Fact:	Apache 2.0.48
Fact:	OpenSSL 0.9.7
Symptom:	OpenSSL ASN.1 Parsing vulnerability in Apache
Symptom:	Server stops responding and an error occurs
Cause:	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.
Fix:	These vulnerabilites are corrected in OpenSSL 0.9.7d. iManager 2.5 ships with OpenSSL 0.9.7d - to resolve the vulnerability upgrading is suggested.

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 reports issue fixed
- 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 iManager 2.0.2

Installation files:

Filename:	eDir_873_webapps.iso
MD5 checksum:	1988608e3c692cc678609a1aea5ecd5f

Service file:

Filename:	Apache.exe (Novell iManager 2.0.2)
MD5 checksum:	02796a89d85fcb5f76825c2f6d115947
Description:	Apache HTTP Server
File version:	2.0.48.0
Product name:	Apache HTTP Server
Product version:	2.0.48
Novell Checksum:	75C5 2724 635D 76F9 1698 01E0

Filename:	Openssl.exe
MD5 checksum:	4a17f1d2cf8b11d2b3ed3b0b8b964d5d
Novell Checksum:	31B7 42E5 E97F 0EB6 D8CC 0C53

OpenSSL ASN.1 Parsing vulnerability in Apache

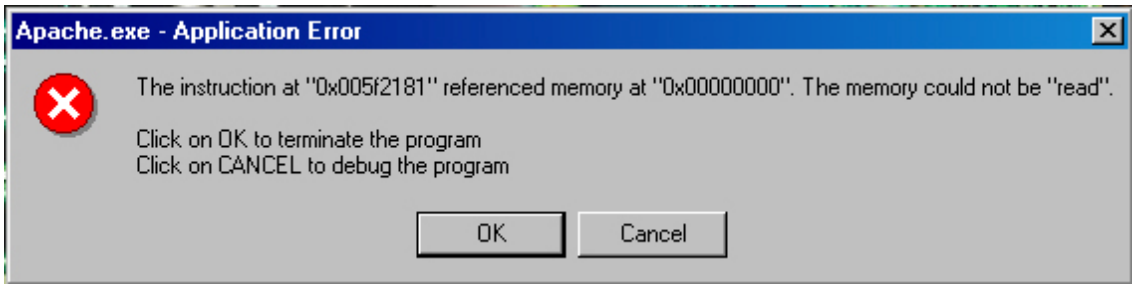
Multiple vulnerabilities were reported in the ASN.1 parsing code in OpenSSL. These issues could be exploited to cause a denial of service or to execute arbitrary code.

The server in this case identifies itself as:
Apache/2.0.48(Win32) mod_ssl/2.0.44 OpenSSL/0.9.7 mod_jk/1.2.4

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

The server will stop responding, and an error will occurs

Following error occurs:



The Service is as default installed on port 8443

Vulnerable version: **Novell iManager 2.0.2**

Corrective actions

These vulnerabilites are corrected in OpenSSL 0.9.7d. iManager 2.5 ships with OpenSSL 0.9.7d - to resolve the vulnerability upgrading is suggested.

Disclaimer