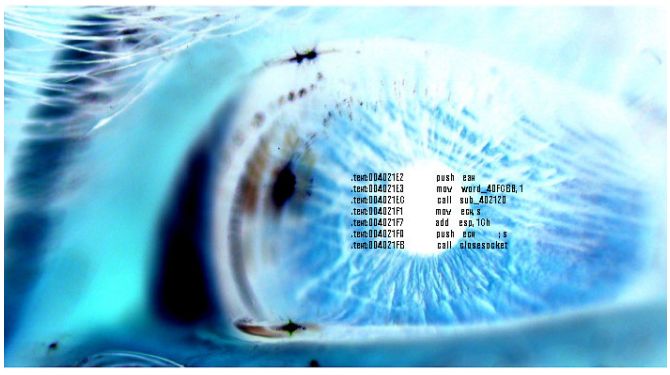
CIRT

Danish Computer Incident Response Team

Security advisory

Sentinel License Manager 7.2.0.2



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

Table of contents

Table of contents 2
Introduction 3
    Problem 3
    What is a Buffer Overflow 3
    Who are SafeNet 3
    What is Sentinel License Manager 3
Timeline of public disclosure 4
Contact information 4
    Public PGP key 4
File description 5
    MD5 software used 5
Sentinel LM 5
    Installation files: 5
    Service files: 5
Technical details of the vulnerabilities 6
    Buffer overflow in the SentinelLM Service 6
Corrective actions 7
Disclaimer 7

Introduction

Problem

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

The Sentinel License Manager 7.2.0.2 software vulnerability:

- Buffer Overflow in SentinelLM service

What is a Buffer Overflow

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Who are SafeNet

http://www.safenet-inc.com/company/index.asp
SafeNet (Nasdaq: SFNT) is a global leader in information security.

SafeNet provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips.

SafeNet technology is the de facto standard in remote access client software and the market leader in USB authentication tokens that eliminate user names and passwords; SSL acceleration devices providing fast and secure online transactions; software security, and licensing products preventing software piracy; high-assurance security products; and SecureIP Technology licensed to Internet infrastructure manufacturers, service providers, and security vendors.

What is Sentinel License Manager

Sentinel LM is a software-based license management application allowing application developers to implement multiple pre-built license models with a single software development integration effort. Developers can sell or deliver multiple license types simply by changing the license file associated with the application sold, reducing development time and facilitating software management of a single code base per release.

Sentinel LM can be deployed with standalone or networked software applications and includes support for many license management models.

http://www.safenet-inc.com/products/sentinel/lm.asp

Timeline of public disclosure

- 06-12-2004 Vulnerability discovered
- 21-12-2004 Research completed
- 29-12-2004 Vendor contacted
- 30-12-2004 Vendor responds that the vulnerability are fixed in version 8.0
- 19-02-2005 Report sent to CERT
- 22-02-2005 Received response from CERT
    - VU#108790
    - CAN-2005-0353
- 07-03-2005 Public disclosure

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

Public PGP key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0

mQGiBEAf2xcRBADMrO7uP0dJq1ZsXkLZLqEhz58LL77qLbXOMNoDRkAo+4MTZoZC
WMNkZsx3D5tbou4KJZCnayt0PFjymyYLsOJ6WauTfXOLA/L+sXTJCa7vSsWwlcQW
m01uy0+djp3XumGHkWdWXvu5cXm7y+UjsF5iiQV8X9EGR18ApoCzA/mi/QCg/zzf
Kw9x7XXGi1pLTpUBI/BvaRkD/2pZf4NLsF7TcCT/rDcNexxr5Ci9xHfglBFKUcQK
9NnF/umLLM3PVyFk8zl7Ra2d8rvPzhDdIi+VGu0Flv5ckRRhiu9A4sOE6zbTkv3f
Q+je/ynnpl36OLswYG+iCELZqzOssRUTe4m9nSeJrbvtyFkW7I/UrBkfursed6yD
vzVDA/4mrWEWgjZkO4wEefwg6FOXr2dChGmdoVXaDyKuQ89hp99THPIALjnorNQK
91IbzyJGX+HaU/KyfKgQfeEEd4znfi9EEaDNDzQmbCntmmCq2PAN0OOcqm4lVNOi
CzEDvsweRxGdffQA+aoNjqeACL1YmPNnTWeNeMNYN7kYD9sTJrQgQ0lSVCBBZHZp
c29yeSA8YWR2aXNvcnlAY2lydC5kaz6JAFgEEBECABgFAkAf2xcICwkIBwMCAQoC
GQEFGwMAAAAACgkQX3fRHNAOUc+KAQCfUD3uwuQmiZjUNXmcKyzXVWFni7cAniIS
fmTQMRf3rIs6kKmSXfnfrXG+uQINBEAf2xcQCAD2Qle3CH8IF3KiutapQvMF6PlT
ETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZ
X9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56N
oKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxbLY7288kj
wEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obE
AxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAIC
B/98f1FQkSzTqoH80viqqJTj3xZVe7xi+n4g4Ji3zuHW+jsgg6SPZOykCDSuzTCO
hJ6LLnwFaqGGu2As7RaNd335P8rH1bLwWQMmIo+Kohj3Ya7cg6gPkkiMSZAIpdca
cXVbxtKZ05dxcixddO2/HOc84/1mR8ajIOsmFKl4DXJ9OwCglgh1i914rQLx5mei
K0XheewAT9eA13yPwbUR1EnormDdaz0USX3l5GBGgvHBO3Xy+muoL8Qzep4PIqfL
Eg18tNXh0vQzBGdmhAjdSVSnSMBts4D5K20HC2YvbdPzWjVeyKg+yTYl4r3r1D+x
vSPng/cCcSX1bESzjOMCE6PDiQBMBBgRAgAMBQJAH9sXBRsMAAAAAAoJEF930RzQ
DlHPdCgAn1jt7gbjHBTQLwTuZH6mpvOnWYs+AJ4sIPIoGz+6/YQLbWr1zXEbmKxo
CA==
=4wBy
-----END PGP PUBLIC KEY BLOCK-----

File description

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

Sentinel LM

Installation files:

Filename:	WCNLM-WCNLM7_2-win32.exe
MD5 checksum:	0bc7f426a468be37938e5ea76e7cae9a

Service files:

Service Name:	SentinelLM
Filename:	LSERVNT.EXE
File version:	7.2.0.2
MD5 checksum:	81a80d785c8145fe85d99da2c756ced2

Technical details of the vulnerabilities

Buffer overflow in the SentinelLM Service

When sending a large amount of data to the SentinelLM service, it will result in a buffer overflow where the Extended Instruction Pointer are overwritten, allowing arbitrary code being run on the server, with the rights of the service.

The Sentinel License Manager is vulnerable to a buffer overflow when sending 3000 bytes of data or more to the UDP port 5093 where the "Lservnt" service are running resulting in the EIP being overwritten allowing arbitrary code execution, with the rights of the service, as default are "SYSTEM".

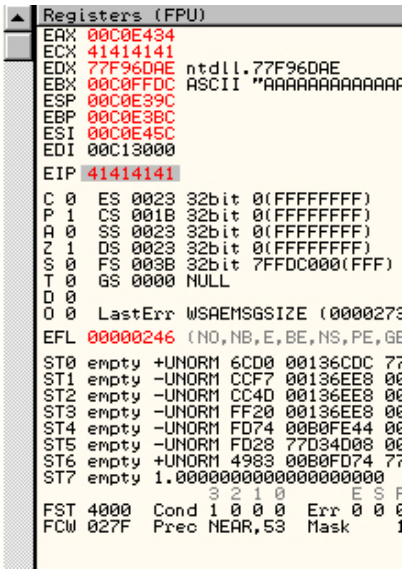


Figure 1 - Taken from OllyDBG

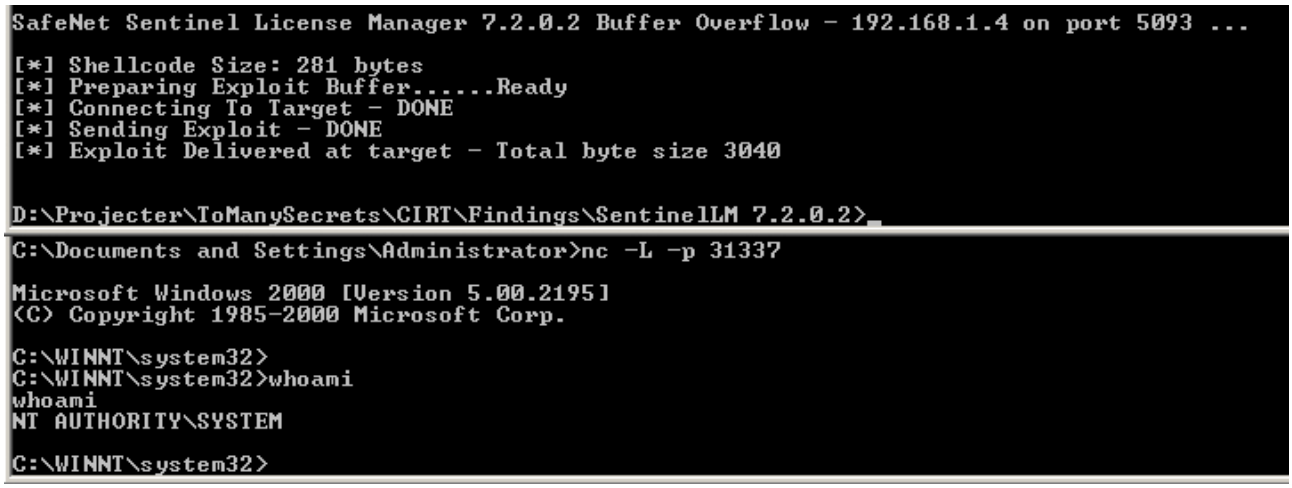


Figure 2 - Shows that remote code execution are possible

Corrective actions

Update to version 8.0 of the Sentinel License Manager.

Disclaimer