

[Full-Disclosure] EEYE: Microsoft ASN.1 Library Length Overflow Heap Corruption

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-02/0506.html>

From: Marc Maiffret (mmaiffret_at_eeeye.com)

Date: 02/10/04

To: <full-disclosure@lists.netsys.com>

Date: Tue, 10 Feb 2004 10:30:47 -0800

Microsoft ASN.1 Library Length Overflow Heap Corruption

Release Date:

February 10, 2004

Date Reported:

July 25, 2003

Severity:

High (Remote Code Execution)

Systems Affected:

Microsoft Windows NT 4.0 (all versions)

Microsoft Windows 2000 (SP3 and earlier)

Microsoft Windows XP (all versions)

Software Affected:

Microsoft Internet Explorer

Microsoft Outlook

Microsoft Outlook Express

Third-party applications that use certificates

Services Affected:

Kerberos (UDP/88)

Microsoft IIS using SSL

NTLMv2 authentication (TCP/135, 139, 445)

Preamble:

We wanted to do another Night Before Xmas but the vendor missed the last few release dates, so we had to resort to our MC(SE).

U Can't Trust This

By: MCSE Hammer

Full-Disclosure: [Full-Disclosure] EEYE: Microsoft ASN.1 Library Length Overflow Heap Corruption

Blaster did ya some harm
We just say, hey, another worm
But thank you, for trusting me
To mind your site's security
It's all good, when your server's downed
Our dope PR will pass blame around
Cuz it's known as such
That this is some software, you can't trust

I told ya Homeland
U can't trust this
Yeah that's why we're giving ya the code
U can't trust this
Check out eEye, man
U can't trust this
Yo let 'em bust more funky system
U can't trust this

Give 'em a string or recvfrom
Like no sweat they got the keys to your kingdom
Now ya know
You talk about eEye, you're talking about holes
Remote and tight
Coders still sweating so someone better write
A book to learn
What it's gonna take in '04
To earn some trust
Legit, either secure or ya might as well quit

That's the word because you know
U can't trust this
U can't trust this

Breakin' in

Stop — eEye time

Description:

eEye Digital Security has discovered a critical vulnerability in Microsoft's ASN.1 library (MSASN1.DLL) that would allow an attacker to overwrite heap memory on a susceptible machine and cause the execution of arbitrary code. Because this library is widely used by Windows security subsystems, the vulnerability is exposed through an array of avenues, including Kerberos, NTLMv2 authentication, and applications that make use of certificates (SSL, digitally-signed e-mail, signed ActiveX controls, etc.).

Technical Description:

The MSASN1 library is fraught with integer overflows. In this advisory, we'll describe a pair of arit