

[NT] Microsoft ASN.1 Library Vulnerability Could Allow Code Execution (MS04-007)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0021.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/11/04

To: list@securiteam.com

Date: 11 Feb 2004 14:23:14 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Microsoft ASN.1 Library Vulnerability Could Allow Code Execution
(MS04-007)

SUMMARY

A security vulnerability exists in the Microsoft ASN.1 Library that could allow code execution on an affected system. The vulnerability is caused by an unchecked buffer in the Microsoft ASN.1 Library, which could result in a buffer overflow.

An attacker who successfully exploited this buffer overflow vulnerability could execute code with system privileges on an affected system. The attacker could then take any action on the system, including installing programs, viewing data, changing data, deleting data, or creating new accounts with full privileges.

Abstract Syntax Notation 1 (ASN.1) is a data standard that is used by many applications and devices in the technology industry for allowing the normalization and understanding of data across various platforms. More information about ASN.1 can be found in Microsoft Knowledge Base Article <<http://support.microsoft.com/default.aspx?scid=kb:en-%20us:252648>> 252648.

Securiteam: [NT] Microsoft ASN.1 Library Vulnerability Could Allow Code Execution (MS04-007)

DETAILS

Affected Components:

- * Microsoft ASN.1 Library

Affected Software:

- * Microsoft Windows NT? Workstation 4.0 Service Pack 6a –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=92400199-B3D5-4826-98D4-F134849F5249&displa>

Download update

- * Microsoft Windows NT Server 4.0 Service Pack 6a –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=E8315430-90CD-4B20-8F54-58527932B588&displa>

Download update

- * Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

–

<http://www.microsoft.com/downloads/details.aspx?FamilyId=D83B39D3-FF13-4D0B-B406-A225AED0D659&di>

Download update

- * Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, Microsoft 2000 Windows Service Pack 4 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=191853C4-A4D2-4797-A8C6-A2E663A53698&displa>

Download update

- * Microsoft Windows XP, Microsoft Windows XP Service Pack 1 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=0CC30297-D4AE-48E9-ACD0-1343D89CCBBA&d>

Download update

- * Microsoft Windows XP 64-Bit Edition, Microsoft Windows XP 64-Bit Edition Service Pack 1 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=383C397F-9318-4AD5-9C2C-0577118A1E68&displa>

Download update

- * Microsoft Windows XP 64-Bit Edition Version 2003, Microsoft Windows XP 64-Bit Edition Version 2003 Service Pack 1 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=FA280168-66E1-4B5F-958F-E178C3F61F7C&displa>

Download update

- * Microsoft Windows Server 2003 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=3D7FFFF9-A497-42FF-90E7-283732B2E117&displa>

Download update

- * Microsoft Windows Server 2003 64-Bit Edition –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=FA280168-66E1-4B5F-958F-E178C3F61F7C&displa>

Download update

Mitigating Factors

In the most likely exploitable scenario, an attacker would have to have direct access to the user's network.

Vulnerability Identifier

Multiple integer overflows in Microsoft ASN.1 library

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0818>

CAN-2003-0818

Workarounds

There are no applicable workarounds. It is highly advisable to download and install the necessary update.

Securiteam: [NT] Microsoft ASN.1 Library Vulnerability Could Allow Code Execution (MS04-007)

Frequently Asked Questions

What is the scope of the vulnerability ?

This is a buffer overrun vulnerability. An attacker who successfully exploited this vulnerability could gain complete control over an affected system. An attacker could take any action on the system, including installing programs, viewing data, changing data, deleting data, or creating new accounts with full privileges.

What causes the vulnerability ?

The vulnerability is caused by an unchecked buffer in the Microsoft ASN.1 Library. If exploited, an attacker could gain system privileges on an affected system.

What is ASN.1 ?

Abstract Syntax Notation 1 (ASN.1) is a data standard that is used by many applications and devices in the technology industry for allowing the normalization and understanding of data across various platforms. ASN.1 has no direct relationship to any specific standard, encoding method, programming language, or hardware platform. It is simply a language for defining standards. Or in other words, standards are written in ASN.1.

A vulnerability exists in Microsoft's ASN.1 implementation that, if exploited, could allow an attacker to cause code to execute remotely with system privileges on an affected system. More information about ASN.1 can be found in Microsoft Knowledge Base Article

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:252648>> 252648.

What might an attacker use the vulnerability to do ?

If successfully exploited, the attacker could be able to take any action on the system, including installing programs, viewing data, changing data, deleting data, or creating new accounts with full privileges.

How could an attacker exploit this vulnerability ?

Because ASN.1 is a standard for many applications and devices, there are many potential attack vectors. To successfully exploit this vulnerability, an attacker must force a computer to decode malformed ASN.1 data. For example, when using authentication protocols based on ASN.1 it could be possible to construct a malformed authentication request that could expose this vulnerability.

What systems are primarily at risk from this vulnerability ?

Server systems are at greater risk than client computers because they are more likely to have a server process running that decodes ASN.1 data.

I'm using Windows NT 4.0. How do I know if I need this update ?

Windows NT 4.0 (Workstation, Server, and Terminal Server Edition) does not install the affected file by default. This file is installed as part of the <<http://www.microsoft.com/technet/security/bulletin/MS03-041.asp>>

MS03-041 Windows NT 4.0 security update and other possible non-security-related hotfixes. If the Windows NT 4.0 security update for <<http://www.microsoft.com/technet/security/bulletin/MS03-041.asp>> MS03-041

Securiteam: [NT] Microsoft ASN.1 Library Vulnerability Could Allow Code Execution (MS04-007)

is not installed, this may not be a required update. To verify if the affected file is installed, search for the file named Msasn1.dll. If this file is present, this security update is required. Windows Update, Software Update Services, and the Microsoft Security Baseline Analyzer will also correctly detect if this update is required.

What does the update do ?

The update removes the vulnerability by modifying the handling of malformed data by the ASN.1 Library.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS04-007.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS04-007.asp>.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.