



Document type: Reference

How to write a Warning or Advisory

(V2.0) October 2006

Keywords

[<Reference, Warning, Advisory, Filtered Warnings>]

Version control

This document may be made available in more than one electronic version or in print. In a case of existing or perceived difference in contents between such versions, the reference version is the version available for download from the WARP Toolbox site <http://www.warp.gov.uk/>

If you find errors in the current document, please send your comment to editor@warp.gov.uk

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

Copyright notification

The copyright and the foregoing restrictions, extend to reproduction in all media. The rights to modify and reproduce are described in the WARP Toolbox terms and conditions described on the WARP Toolbox site.

Contents

1	Scope	2
2	References	2
3	Definitions and abbreviations	2
3.1	Definitions	2
3.2	Abbreviations.....	3
4	Background	3
5	The anatomy of a security vulnerability.....	4
5.1	Undisclosed vulnerabilities.....	4
5.2	Vendor discovered and disclosed vulnerabilities.....	4
5.3	Vulnerabilities discovered by third parties	5
5.4	Engineering an exploit.....	6
6	A real advisory	6
6.1	The vulnerability is announced.....	6
6.2	The situation evolves	7
7	Writing a WARP Advisory	7
7.1	The WARP Advisory.....	7
7.2	Revisions.....	9
8	Conclusion	10
	Appendix A – Microsoft Advisory MS04-007.....	11
	Appendix B – US-CERT TA04-041A	13
	Appendix C – UNIRAS brief 75/04	16
	Appendix D – The WARP Advisory.....	18
	History	19

1 Scope

This document describes, by means of an illustrated example, the typical thought processes behind the creation of a WARP advisory that would be forwarded to WARP members by the Filtered Warnings service. The document describes:

- The processes by which vulnerabilities are found and fixed;
- How information changes over time;
- The kind of information that should be supplied to WARP members.

Potential WARP operators can use this guide to access their capability to perform the required tasks, and to assist in the creation of local procedures and policies.

2 References

For the purposes of this Report, the following references apply:

- [1] [Microsoft Advisory MS04-007](#)
- [2] [eEye Digital Security Advisory AD20040210](#)
- [3] [US-CERT Cyber Advisory TA04-041A](#)
- [4] [UNIRAS Brief 75/04](#)

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply:

CERT:	Computer Security Incident Response Team, based on the model developed by the Carnegie Mellon University.
Exploit:	A detailed procedure for exploiting a vulnerability to give a result desirable to an attacker, and (usually) undesirable to the owner of the system.
Third-party:	Somebody other than the Vendor, or the organisation that owns a product.
UNIRAS:	The UK government CERT.
Vendor:	Producer of a product, be they a commercial organisation or an Open Source community.
Vulnerability	A bug in a computer program, operating system or protocol that in some way exposes a system to undesired manipulation.

XML Schema: The definition of field names and their data types that an XML document will implement. The XML schema explains to a consumer (be it a person or a computer program) what fields could be expected in a corresponding XML document based on the schema.

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

FWA: Filtered Warnings Application
NISCC: National Infrastructure Security Co-ordination Centre
UNIRAS: Unified Incident Reporting and Alert Scheme (UK Gov. CERT)
WARP: Warning, Advice and Reporting Point

4 Background

The WARP Filtered Warnings service provides WARP members with a feed of security related information that is filtered based upon their own requirements. Typically security information sources provide a great deal of information, and no one person is going to be interested in it all. In order to rationalise the information, the WARP operator needs to be able to categorise the information received, allowing it to be fed on to only those WARP members that are interested.

A secondary task that the WARP operator performs is the aggregation of information sources. Many sources will provide information on the same technical vulnerability. The central position of the WARP operator between the information sources and the WARP community allows the information from various sources to be combined into a single warning. This aggregation activity can provide real value, and potentially prevent the proliferation of false alarms to the WARP community.

In order to assist in the distribution of warnings and alerts to WARP members based on subscription profiles, NISCC has made the Filtered Warnings Application available. As part of the initiative to develop this application, a XML schema was created that includes the fields thought most likely to be required in order to specify typical warnings and advisories. When writing an advisory, the WARP administrator needs to know how these fields relate, and the WARP members may also need an understanding of which fields contain the information they are interested in. It is not necessary to run the Filtered Warnings Application in order to operate the Filtered Warnings Service. All the discussions in this document are still relevant, no matter how the WARP chooses to distribute information.

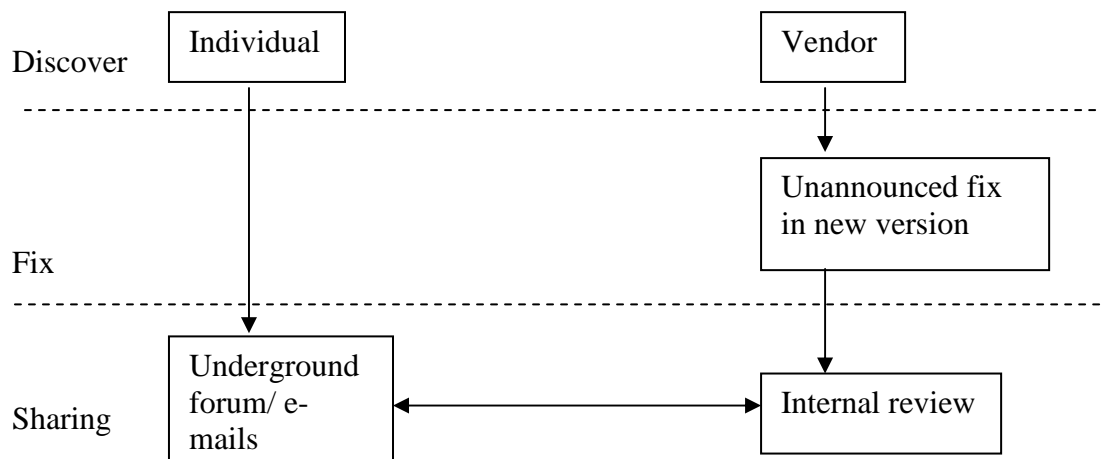
5 The anatomy of a security vulnerability

Security vulnerabilities probably exist in all operating systems, applications and network protocols (which we will collectively call “products”) generally in use today. Depending upon the environment in which a product is used, the security vulnerabilities it contains may never be found. Generally, in the modern networked world, security vulnerabilities will be found in products that are in general public use. How a security vulnerability is published largely depends upon who identifies it. The following sections describe some likely scenarios.

5.1 Undisclosed vulnerabilities

Undisclosed vulnerabilities are dangerous, and would be difficult for a WARP organisation to find out about. An undisclosed vulnerability has not been publicly reported, but that does not mean that nobody knows about it. Clearly the individual or organisation that finds the vulnerability is fully aware of the situation. They may share the information with others behind closed doors, thus spreading the knowledge, but still not informing those that stand to suffer from the vulnerability. The following diagram illustrates the sources via which undisclosed vulnerabilities can be discovered, shared and fixed.

Figure 1 – Undisclosed vulnerabilities

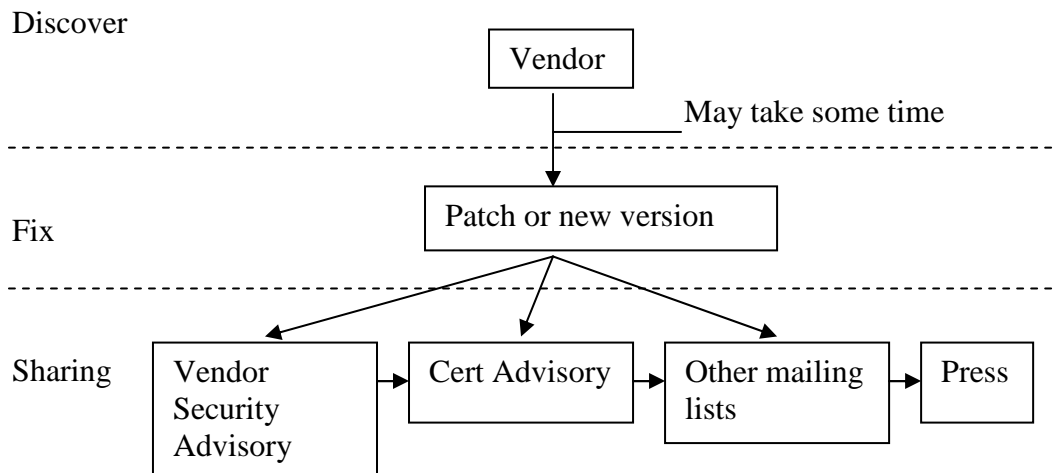


Whilst undisclosed vulnerabilities are not something the WARP would be expected to deal with, it is worth understanding that they can and do exist.

5.2 Vendor discovered and disclosed vulnerabilities

Vendors should continuously be looking to improve the security of their products, and when enhancements are available they will generally notify their users via a mailing list specific to their products. Additionally, in order to improve the reach of the information, vendors may notify more general security mailing lists, and national CERT organisations. Where a CERT is involved, they will usually rate the supplied information in some way, and where the vulnerability is deemed to be readily exploitable, may make a high priority announcement. Ultimately the general press may also be interested, but they are unlikely to be notified by the vendors themselves.

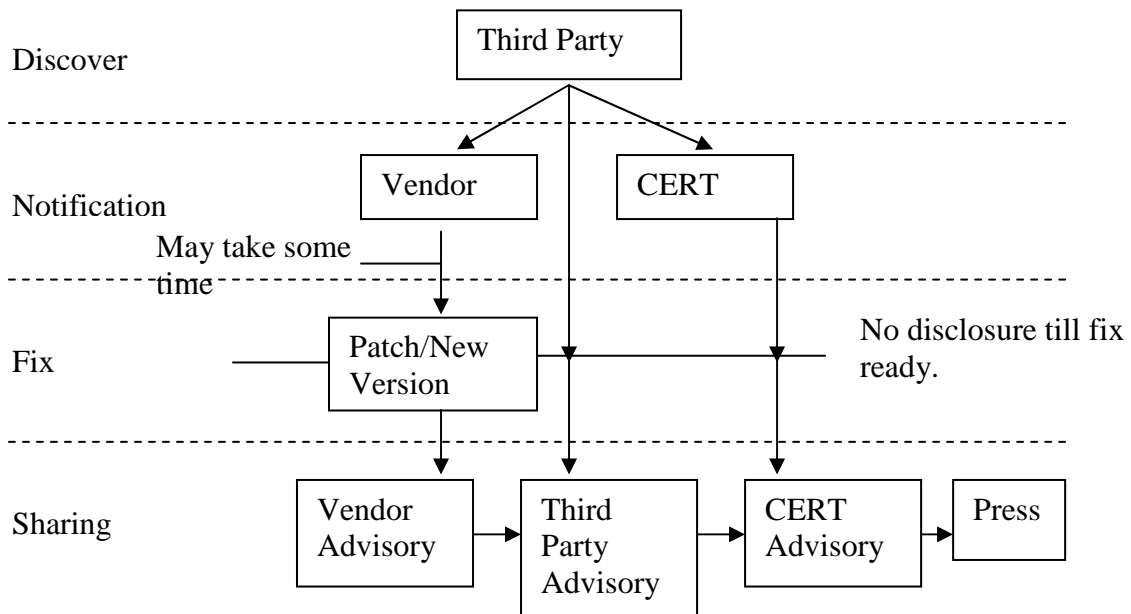
Figure 2 – Vendor discovered vulnerabilities



5.3 Vulnerabilities discovered by third parties

Where a security vulnerability is discovered by a third party, the vendor and their customers rely entirely on the integrity of the individual or organisation involved. The main difference between this section and section 5.1 is that rather than keeping to a closed community for their own purposes, the discoverer wishes to reveal the information they have discovered in order to ensure a fix is produced. This process is often called Full Disclosure. It is generally accepted that the product vendor should be given every opportunity to fix an issue before the discoverer “goes public”. For the vendor’s part, they are expected to be responsive to third-parties reporting security issues with their products.

Figure 3 – Third party discovered vulnerabilities



Sometimes a third party will report a vulnerability to a vendor, and then, due to lack of action from that vendor, will go public without a fix being available. This technique has been seen to shock slow vendors into action in the past, but is generally regarded as somewhat irresponsible by owners of vulnerable software.

5.4 Engineering an exploit

An exploit – the capability to use a security vulnerability to make some undesired behaviour happen – is often not developed at the same time the vulnerability is identified. It is generally obvious to skilled technicians which vulnerabilities will be easily exploitable; actually producing the exploit is not necessary. Once a vulnerability has been made public, it must be assumed that an exploit will be generally available shortly after. This means the window for patching vulnerable software is small, and reducing all the time. It must also be remembered that where a vulnerability is found and kept secret, the exploit could also be secretly developed.

6 A real advisory

Given the information in Section 5, it is easy to see why a single security vulnerability may:

- Give rise to more than one advisory from more than one source;
- Be updated over time;
- Be time critical – must be rapidly disseminated.

In this section these principles are illustrated by working through a real example relating to a Microsoft advisory issued in February 2004.

6.1 The vulnerability is announced

Microsoft vulnerability MS04-007 was announced on the 10th February 2004. Most of the vulnerability text is reproduced in Appendix A – Microsoft Advisory MS04-007. In the ‘Acknowledgements’ section you will notice that Microsoft thanks eEye Digital Security for bringing the vulnerability to their attention. On the same day eEye published their own information regarding the vulnerability, which is published on their website as eEye advisory [AD20040210](#). The text of the eEye advisory has not been included in this document, but if you follow the above link you will find, as is often the case, that the information provided by the discoverer of the vulnerability is much more detailed and complete than that provided by the Vendor.

Additional items of interest in the eEye advisory include the fact that the problem was reported to Microsoft in July 2003 (it seems Microsoft took six months to produce a patch). The eEye text also includes some very helpful pointers as to exactly which services are exploitable due to this issue, and goes on to give an in depth discussion of how an exploit might work, listing in detail the vulnerable functions.

Tip: Always take a look at the advisory from the originator of the vulnerability in addition to any vendor announcement – you may discover more information.

Both the Microsoft and the eEye alert listed the vulnerability as “Critical”, as the problem uncovered would allow a system to be exploited remotely via the network. Under these circumstances a WARP running the Filtered Warnings service would be expected to pass the information on to their community as quickly as possible, by creating their own advisory as described in section 7. Additional proof as to the urgency of this vulnerability

is provided when the US-CERT issues a Technical Cyber Security Alert, also on 10th February 2004, urging the relevant patches be applied as soon as possible (see Appendix B – US-CERT TA04-041A). US-CERT tends to only issue these alerts with good reason.

Tip: If you are unsure how critical a vulnerability announcement may be, look for corroboration from more than one trusted source.

6.2 The situation evolves

Clearly the information from the previous section will have caused the creation of a WARP advisory, and hopefully the WARP membership will be taking steps to ensure the vulnerable systems in their environments are patched. The situation does not end here though. As was discussed in section 5.4, once a vulnerability is announced, it is only a matter of time before an exploit is produced. UNIRAS, the UK government CERT, announces on the 14th February 2004 that exploit code for this vulnerability is now known to be available (see Appendix C – UNIRAS brief 75/04).

The known availability of an exploit for a critical vulnerability is a very good reason to revise a WARP advisory and reissue it, giving the WARP community vital additional information that they may need to ensure patching gets the priority it deserves.

7 Writing a WARP Advisory

WARPs that operate a Filtered Warnings service provide two functions for their community. Firstly, they enable their membership to elect to receive information about only systems that interest them. Secondly, they have the ability to add value to the warning distribution process, by including additional information, or aggregating information from many sources.

In the scenario outlined in section 6, it is possible for the WARP administrator to review the Microsoft and the eEye advisories, as well as the information flagged by US-CERT. By taking these three reports into account, it is clear that patching the Microsoft ASN.1 vulnerability is extremely urgent as:

- US-CERT have issued an urgent advisory
- eEye have supplied a detailed analysis of the vulnerability, and stated that it is easy to remotely exploit
- Some significant time has passed between the Vendor being notified and a patch being issued.

Clearly, not all advisories will have this kind of profile, but this example shows circumstances under which the WARP administrator can add value by wording an advisory to their membership that has greater urgency than the one penned by the vendor.

7.1 The WARP Advisory

The following shows an example WARP Advisory that could be produced based on the information known about the Microsoft ASN.1 vulnerability on the 10th February 2004.

The advisory is split into the sections that are used by the Filtered Warnings Application, but there is no requirement to use the Filtered Warnings Application to run a Filtered Warnings service.

Title: MS04-007 – Microsoft ASN.1 Vulnerability. Urgent patching required for Windows NT, 2000, XP and 2003

Tip: The Title field is used by FWA as the E-mail subject, so if the advisory is urgent, make sure the Title information gives this impression.

Severity: Critical

Tip: Try to reserve the critical severity for the worst problems that will affect the most users. This will ensure the WARP members take note of these advisories.

Categories: Windows 2000, Windows XP, Windows 2003

Tip: The FWA system will generate this field based on tree selections. The categories chosen will depend on your own procedures.

Specific-Software-Affected: All editions of Windows 2000, Windows XP and Windows 2003 Server

Tip: Provide clarification that may not be possible with your category selection.

Source: Microsoft Inc.

Tip: Use the most credible source in this field. If there is a vendor advisory, use the vendor.

Impact: Remote system compromise

Tip: Give the reader the “worse case scenario” as succinctly as possible.

Also known as: Q828028, eEye Advisory AD20040210, US-CERT TA04-041A

Tip: Include references to all other sources used.

Description Field:

Description:

Multiple integer overflow vulnerabilities in the Microsoft Windows ASN.1 parser library could allow an unauthenticated, remote attacker to execute arbitrary code with SYSTEM privileges. All installations of Windows NT, Windows 2000, Windows XP and Windows 2003 are vulnerable. The vendor announcement can be viewed at <http://www.microsoft.com/technet/security/bulletin/ms04-007.msp>.

Tip: Clearly the description could be far more technical and involved, but it is better to keep it more general, and provide a link to the detail. Wholesale reproduction of the original advisories should be avoided.

Exploit:

Currently there are no known exploits in the wild, however due the length of time the vendor has taken to produce the fix, and the amount of detail available regarding the problem and how it could be exploited, it is considered to be extremely likely that an easy to use exploit script will be available shortly.

Tip: Where there is no exploit information currently available the WARP administrator must use judgement to give the community advice.

Workaround:

Apply patches to vulnerable systems as soon as possible. Patches for all vulnerable operating system versions can be obtained from Microsoft Inc. via this URL: <http://www.microsoft.com/technet/security/bulletin/ms04-007.msp>.

Members should also follow good network security techniques, and ensure that network access to and from all systems is restricted to only that which is required for on going operations. This should NOT be considered an alternative to patching.

Tip: Tell the WARP members what they should do. Do not assume they will realise!

7.2 Revisions

It would be hoped that in response to this advisory, the WARP members will galvanise their various organisations into action, and patching will commence as quickly as possible. When significant new information becomes available, in this case the known availability of exploit code, the WARP administrator can provide an additional or updated advisory. The WARP members may well appreciate this additional information.

If a manual system of advisory distribution is being used, it may be necessary to create a completely new advisory to cover this update. The Filtered Warnings Application allows a previously sent advisory to be revised and reissued, so only revision notes need be created.

Revision Notes:

Please be aware that exploit code has now been published on the Internet. The published code is designed to create a denial of service attack against Windows 2000 and later systems. It is highly likely this code will be adapted by others and more attack types created. Please implement the advice shown in the workaround section urgently.

Tip: The revision notes are distributed along with the original advisory information, so you can refer to the rest of the advisory.

8 Conclusion

The previous sections have shown that, by understanding the means by which product vulnerabilities are found and reported, it is possible to examine the advisories produced with a good degree of insight. This can be passed on to the WARP membership most effectively by:

- Accurately pitching the sense of urgency based on knowledge of the requirements of the WARP community;
- Collating information from multiple sources;
- Updating the community when the situation changes;
- Providing consistency in how the various advisory fields are utilised.

Appendix A – Microsoft Advisory MS04-007

The following text is taken from the Microsoft Advisory regarding this vulnerability. Only the first section of the advisory is shown, the full text can be found at <http://www.microsoft.com/technet/security/bulletin/ms04-007.msp>.

Microsoft Security Bulletin MS04-007

ASN.1 Vulnerability Could Allow Code Execution (828028)

Issued: February 10, 2004

Version Number: 1.0

Summary

Who should read this document:

Customers who are using Microsoft® Windows®

Impact of vulnerability:

Remote Code Execution

Maximum Severity Rating:

Critical

Recommendation:

Systems administrators should apply the update immediately.

Security Update Replacement:

None

Caveats:

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 [MS03-041](#) Windows NT 4.0 security update and other possible non-security-related hotfixes. If the Windows NT 4.0 security update for [MS03-041](#) 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.

Tested Software and Security Update Download Locations:

Affected Software:

- Microsoft Windows NT® Workstation 4.0 Service Pack 6a - [Download the update](#).
- Microsoft Windows NT Server 4.0 Service Pack 6a - [Download the update](#).
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 - [Download the update](#).
- Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4 - [Download the update](#).

- Microsoft Windows XP, Microsoft Windows XP Service Pack 1 - [Download the update](#).
- Microsoft Windows XP 64-Bit Edition, Microsoft Windows XP 64-Bit Edition Service Pack 1 - [Download the update](#).
- Microsoft Windows XP 64-Bit Edition Version 2003, Microsoft Windows XP 64-Bit Edition Version 2003 Service Pack 1 - [Download the update](#).
- Microsoft Windows Server™ 2003 - [Download the update](#).
- Microsoft Windows Server 2003 64-Bit Edition - [Download the update](#).

Tested Microsoft Windows Components:

Affected Components:

- Microsoft ASN.1 Library

The software listed above has been tested to determine if the versions are affected. Other versions either no longer include security update support or may not be affected. Please review the [Microsoft Support Lifecycle](#) Web site to determine the support lifecycle for your product and version.

Acknowledgments

Microsoft [thanks](#) the following for working with us to help protect customers:

- [eEye Digital Security](#) for reporting the issue in [MS04-007](#)

Appendix B – US-CERT TA04-041A

The US-CERT issued Technical Cyber Security alert TA04-041A on 10th February 2004.

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Multiple Vulnerabilities in Microsoft ASN.1 Library

Original issue date: February 10, 2004
Last revised: --
Source: US-CERT

A complete revision history is at the end of this document.

Systems Affected

- * Microsoft Windows NT 4.0
- * Microsoft Windows NT 4.0 TSE
- * Microsoft Windows 2000
- * Microsoft Windows XP
- * Microsoft Windows Server 2003

Overview

Multiple integer overflow vulnerabilities in the Microsoft Windows ASN.1 parser library could allow an unauthenticated, remote attacker to execute arbitrary code with SYSTEM privileges.

Description

Microsoft Security Bulletin MS04-007 announces a patch for multiple vulnerabilities in the Microsoft Windows ASN.1 library (msasn1.dll). According to information from eEye Digital Security, the vulnerabilities involve integer overflows and other flaws in integer arithmetic. The latest version of this document can be found at

<<http://www.us-cert.gov/cas/techalerts/TA04-041A.html>>

Additional information is available in two vulnerability notes:

VU#216324 - Microsoft ASN.1 Library improperly decodes malformed ASN.1 length values
(Other resources: AD20040210, MS04-007, CAN-2003-0818)

VU#583108 - Microsoft ASN.1 Library improperly decodes constructed bit strings
(Other resources: AD20040210-2, MS04-007, CAN-2003-0818)

eEye has published two detailed advisories on these issues: AD20040210 and AD20040210-2.

Any application that loads the ASN.1 library could serve as an attack vector. In particular, ASN.1 is used by a number of cryptographic and authentication services such as digital certificates (x.509),

Kerberos, NTLMv2, SSL, and TLS. Both client and server systems are affected. The Local Security Authority Subsystem (lsass.exe) and a component of the CryptoAPI (crypt32.dll) use the vulnerable ASN.1 library.

Impact

An unauthenticated, remote attacker could execute arbitrary code with the privileges of the process using the ASN.1 library. In the case of most server and authentication applications, an attacker could gain SYSTEM privileges.

Solution

Apply a patch

Apply the appropriate patch as specified by Microsoft Security Bulletin MS04-007.

Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

Please see Microsoft Security Bulletin MS04-007.

References

- * Vulnerability Note VU#216324 -
<<http://www.kb.cert.org/vuls/id/216324>>
- * Vulnerability Note VU#583108 -
<<http://www.kb.cert.org/vuls/id/583108>>
- * eEye Digital Security Advisory AD20040210 -
<<http://www.eeye.com/html/Research/Advisories/AD20040210.html>>
- * eEye Digital Security Advisory AD20040210-2 -
<<http://www.eeye.com/html/Research/Advisories/AD20040210-2.html>>
- * Microsoft Security Bulletin MS04-007 -
<<http://microsoft.com/technet/security/bulletin/MS04-007.asp>>
- * Microsoft Knowledge Base Article 252648 -
<<http://support.microsoft.com/default.aspx?scid=252648>>

These vulnerabilities were researched and reported by eEye Digital Security. Information from eEye and Microsoft was used in this document.

Feedback can be directed to the author, Art Manion.

Copyright 2004 Carnegie Mellon University.

Revision History

February 10, 2004: Initial release

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)

iD8DBQFAKVrdXlvNRxAkFWARAUovAJwL2gJJPBRdrtZ0Le4yyLQLu7CHewCgvaCW
5hU8LQ/oOC4sI8PpnkppCyg=
=0e/N
-----END PGP SIGNATURE-----

Appendix C – UNIRAS brief 75/04

-----BEGIN PGP SIGNED MESSAGE-----

UNIRAS (UK Govt CERT) Briefing Notice - 75/04 dated 14.02.04 Time: 19:50
UNIRAS is part of NISCC(National Infrastructure Security Co-ordination Centre)

UNIRAS material is also available from its website at www.uniras.gov.uk and
Information about NISCC is available from www.niscc.gov.uk

Title

=====

Exploit code for Microsoft Windows ASN.1 Vulnerabilities

Detail

=====

Further to Uniras Brief 63/04 and Alert 04/04, departmental and organisational security officers should be aware that exploit code has been published on the Internet.

This exploit has been published as commented source code and claims to create a Denial of Service (DoS) condition in the LSASS process on the target computer. Examination of the source code indicates that it causes this DoS by sending a malformed NetBIOS message to TCP port 139 or 445. It is apparently written to operate against Windows 2000 and later platforms.

Whilst NISCC has not compiled and tested this exploit code, a code review indicates that it is likely to operate successfully. A good knowledge of Windows programming would be required to take this code a step further in order to return a shell on the target computer, and therefore take full control of it. It should be noted, however, that the original researchers of these vulnerabilities, eEye Digital Security, claim that they have achieved remote system compromise after developing and executing proof of concept exploits.

Mitigation against this specific exploit is consistent with established good practice of blocking access to TCP ports 139 and 445 from untrusted networks. Further information on mitigation and patches is available from the Microsoft advisory located at:
<http://www.microsoft.com/technet/security/bulletin/MS04-007.asp>.

For additional information or assistance, please contact the HELP Desk by telephone or Not Protectively Marked information may be sent via EMAIL to:
uniras@niscc.gov.uk

Office Hours:

Mon - Fri: 08:30 - 17:00 Hrs
Tel: +44 (0) 20 7821 1330 Ext 4511
Fax: +44 (0) 20 7821 1686

Outside of Office Hours:

On Call Duty Officer:
Tel: +44 (0) 20 7821 1330 and follow the prompts

This Briefing contains the information released by the original author. Some of the information may have changed since it was released. If the vulnerability affects you, it may be prudent to retrieve the advisory from the canonical site to ensure that you receive the most current information concerning that problem.

Reference to any specific commercial product, process, or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by UNIRAS or NISCC. The views and opinions of authors expressed within this notice shall not be used for advertising or product endorsement purposes.

Neither UNIRAS or NISCC shall also accept responsibility for any errors or omissions contained within this briefing notice. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

UNIRAS is a member of the Forum of Incident Response and Security Teams (FIRST) and has contacts with other international Incident Response Teams (IRTs) in order to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing amongst its members and the community at large.

<End of UNIRAS Briefing>

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0

iQCVAwUBQC6DF4pao72zK539AQG4IQQAi8o4acLJY7UpF16VtQ3gDN3yvbHYmIK
z1UU5LkO3M7zC2jCh7RPAXfsoxpnFYfbrmTWYqAadTx6ws54MCjqlEhM79wbw73D
qYHJrOOfjk75ALTY0rt10F7XcdBYKmMXW0NXl2lBEZ+YNMMEfgwhni53Cbks//V
mttYMyXNzws=
=pWwL

-----END PGP SIGNATURE-----

Appendix D – The WARP Advisory

Critical Rated Advisory

Source: Microsoft Inc.

Feb 10 2004 4:19PM

Categories: Windows 2003, Windows XP, Windows 2000

Software Affected: All editions of Windows 2000, Windows XP and Windows 2003 Server

MS04-007 – Microsoft ASN.1 Vulnerability. Urgent patching required for Windows NT, 2000, XP and 2003

Also Known As: Q828028, eEye Advisory AD20040210, US-CERT TA04-041A

Impact: Remote system compromise

Description:

Multiple integer overflow vulnerabilities in the Microsoft Windows ASN.1 parser library could allow an unauthenticated, remote attacker to execute arbitrary code with SYSTEM privileges. All installations of Windows NT, Windows 2000, Windows XP and Windows 2003 are vulnerable. The vendor announcement can be viewed at <http://www.microsoft.com/technet/security/bulletin/ms04-007.msp>

Exploit:

Currently there are no known exploits in the wild, however due the length of time the vendor has taken to produce the fix, and the amount of detail available regarding the problem and how it could be exploited, it is considered to be extremely likely that an easy to use exploit script will be available shortly.

Workaround:

Apply patches to vulnerable systems as soon as possible. Patches for all vulnerable operating system versions can be obtained from Microsoft Inc. via this URL: <http://www.microsoft.com/technet/security/bulletin/ms04-007.msp>.

Members should also follow good network security techniques, and ensure that network access to and from all systems is restricted to only that which is required for on going operations. This should NOT be considered an alternative to patching.

Thank you for using the Filtered Warnings Application

History

Version	Date	Description
V1.0	4 June 2004	First issue
V1.1	21 June 2004	Changes include those requested by an external reviewer and judged to be significant.
V2.0	13 October 2006	Second issue, made less FWA specific and updated to reflect the fields available in FWA V4.1.