

NHS Information Governance:

Technical Security

Technology Bulletin: Microsoft Internet Explorer Security Vulnerability – 979352 – “Aurora”

Department of Health Informatics Directorate

January, 2010

Amendment History

Version	Date	Amendment History
0.1	20 th January, 2010	First draft for comment
0.2	21 st January, 2010	Second draft following peer review
1.0	21 st January, 2010	Approved by NHS Head of IT Security

Introduction

On 14th January, 2010, Microsoft released a security advisory detailing a vulnerability in multiple versions of Internet Explorer which could be used to compromise various versions of the Windows operating system.

This bulletin has been written to advise NHS organisations of the specific details of the vulnerability available at this time and to provide guidance as to mitigating actions which can be taken to reduce the risk of exploitation of this vulnerability on NHS computer systems.

Microsoft's security advisory on this issue can be found here:

<http://www.microsoft.com/technet/security/advisory/979352.mspx>

Issue Details

A vulnerability exists in multiple versions of Internet Explorer which can be exploited to run unauthorised/malicious code on various versions of Windows. The table below provides information as to which versions of Internet Explorer and which versions of the Windows operating system are affected.

	Windows 2000	Windows XP	Windows Server 2003	Windows Vista	Windows 7	Windows Server 2008 ¹
Internet Explorer 5.01 SP4	✓	N/A	N/A	N/A	N/A	N/A
Internet Explorer 6	✓	✓	✓	N/A	N/A	N/A
Internet Explorer 7	N/A	✓	✓	✓	N/A	✓
Internet Explorer 8	N/A	✓	✓	✓	✓	✓

(Note that all OS architectures (32 bit and 64 bit) are affected as well as all applicable Service Packs.)

The vulnerability is manifested as an invalid pointer reference to an object which has been previously deleted. Under certain circumstances, it is possible to reference the invalid pointer and so allow remote execution of malicious code.

In order to exploit this vulnerability, an attacker would need to coerce a user into visiting a malicious web site or other web site which had been compromised with suitable attack code (such sites can include those which allow user contributions such as blogs, forums and so forth). Typically, this would be done by including a link in an e-mail or on a web page which would entice the user into visiting the compromised or malicious web site.

A number of targeted attacks using this vulnerability have been leveraged against a number of large organisations.² At this time, these attacks have been aimed solely at specific organisations and

¹ 'Server Core' installation not affected.

² More information on these attacks, dubbed 'Operation: Aurora' by the technology press can be found here: <http://blogs.zdnet.com/security/?p=5259>

currently only affect **Internet Explorer 6 on the Windows 2000 and Windows XP platforms**. However, work is ongoing to leverage the exploit code so that it works successfully on other versions of Internet Explorer on other Windows platforms.

Risks

Exploitation of this vulnerability could allow for complete compromise of the affected system. This could allow an attacker to download and install further malware/spyware on to the computer, add user accounts to the computer, steal sensitive data held locally and centrally and so forth. Users whose accounts have fewer privileges on the targeted system are likely to be less affected than those whose accounts have privileges equivalent to the 'local administrator'.

It is also possible that exploiting this vulnerability could allow for the compromised computer to be used as a 'staging point' for further attacks against other computer systems including those outside of the organisation.

If an organisation has systems compromised via this vulnerability, there may be consequential reputational damage, especially if sensitive data is affected or the compromised system is used to attack other systems.

Guidance

Microsoft will post a security update to resolve this vulnerability. The update will be obtainable from: <http://www.microsoft.com/technet/security/bulletin/ms10-jan.msp> or from Windows Update (<http://windowsupdate.microsoft.com>). Organisations with system management software/patch management software should use these products to obtain the relevant update.

It is recommended that this update is applied to all affected computers within an organisation. Organisations should ensure that appropriate levels of testing of the update take place prior to mass deployment. Organisations should be satisfied that the update does not cause any problems with already existing applications and so forth prior to applying it to all affected systems. Where problems are discovered, organisations should contact Microsoft and/or the vendor of the application/product with the problem and consider applying one of the mitigating actions from the Microsoft Security Advisory related to this issue instead.

On systems where the update cannot be applied, Microsoft offers a number of mitigations which may help to reduce the possibility of successful attacks. It must be noted however that these mitigations do not resolve the vulnerability, only make it harder to exploit and therefore the recommended approach is to apply the update. Further information on these mitigations can be found within the 'Workarounds' section of the applicable Microsoft Security Advisory here: <http://www.microsoft.com/technet/security/advisory/979352.msp>

It is additionally further recommended that organisations still using Internet Explorer 6 on the affected platforms upgrade to Internet Explorer 7. Internet Explorer 7 has been warranted to work correctly with SPINE applications such as CSA and provides additional security features over Internet Explorer 6. Further information on Internet Explorer 7 including methods for deployment across an organisation can be found here: <http://www.microsoft.com/uk/windows/products/winfamily/ie/default.msp>

Further assistance

If further assistance or guidance is required on this or any other technical security related issue, please contact the Department of Health Informatics Directorate Infrastructure Security Team at: cfh.infosecteam@nhs.net