



State of Alaska
State Security Office

Department of Administration
Enterprise Technology Services

State of Alaska Cyber Security &
Critical Infrastructure Cyber Advisory

June 01, 2009

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

SA2009-028

DATE(S) ISSUED:

06/01/09

Subject:

Vulnerability in Microsoft DirectX Could Allow Remote Code Execution

Source:

MS-ISAC / Microsoft

Systems Affected:

- DirectX 7.0 on Microsoft Windows 2000 Service Pack 4
- DirectX 8.1 on Microsoft Windows 2000 Service Pack 4
- DirectX 9.0, 9.0a, 9.0b, 9.0c on Microsoft Windows 2000 Service Pack 4
- DirectX 9.0, 9.0a, 9.0b, 9.0c on Windows XP Service Pack 2 and Windows XP Service Pack 3
- DirectX 9.0, 9.0a, 9.0b, 9.0c on Windows XP Professional x64 Edition Service Pack 2
- DirectX 9.0, 9.0a, 9.0b, 9.0c on Windows Server 2003 Service Pack 2
- DirectX 9.0, 9.0a, 9.0b, 9.0c on Windows Server 2003 x64 Edition Service Pack 2
- DirectX 9.0, 9.0a, 9.0b, 9.0c on Windows Server 2003 with SP2 for Itanium-based Systems

Overview:

A vulnerability has been discovered in Microsoft DirectX that could allow a remote attacker to take complete control of a vulnerable system. DirectX is an application within Microsoft Windows used to stream various types of media and enables graphics and sound when playing games or watching video. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Microsoft has recommended three workarounds, each of which has a different level of impact. The first is to disable QuickTime parsing via DirectX. This is the Microsoft recommended method as it still allows Windows Media Player to play other media and only stops QuickTime from playing. The second is to set the Kill-Bit WMP in ActiveX. This will mitigate current attacks against Internet Explorer, but does not provide protection against other attack vectors. The third is to unregister/ACL the quartz.dll. This method provides the same level of protection as the first method. However there is a greater impact on use as all media files will fail to play in applications (i.e. Internet Explorer, Windows Media Player) which use DirectX.

Currently, there are no patches available for this vulnerability and there are reports of targeted attacks exploiting this issue on the Internet.

Recommendations / Resolution:

- After testing, apply the appropriate patch provided by Microsoft to vulnerable systems as soon as it becomes available. Consider applying the workarounds that are provided by Microsoft. <http://support.microsoft.com/kb/971778>
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Ensure that all anti-virus software is up to date with the latest signatures.
- Consider blocking QuickTime media at your proxy server and email gateways.
- Do not open email attachments from unknown or un-trusted sources.

References:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/971778.msp>

<http://support.microsoft.com/kb/971778>

<http://blogs.technet.com/msrc/archive/2009/05/28/microsoft-security-advisory-971778-vulnerability-in-microsoft-directshow-released.aspx>

<http://blogs.technet.com/srd/archive/2009/05/28/new-vulnerability-in-quicktime-parsing.aspx>

Security Focus:

<http://www.securityfocus.com/bid/35139>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1537>

Secunia:

<http://secunia.com/advisories/35268/>