



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory
January 9, 2007**

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:

2007-03

DATE ISSUED:

01/09/2007

SUBJECT:

Vulnerability in Vector Markup Language Affecting Microsoft Window Platforms

OVERVIEW:

Microsoft has released Microsoft Security Bulletin MS07-004 which addresses a new vulnerability in multiple versions of Microsoft Windows. If successfully exploited, this vulnerability could allow for a remote attacker to execute arbitrary programs on the system with the current user's privileges. Microsoft has confirmed reports of widespread use of these exploits in the wild.

Vulnerable systems can be exploited by visiting malicious web sites with Internet Explorer or by viewing malicious HTML email messages in Outlook.

Note that this patch replaces the patch released with the Microsoft Security Bulletin MS06-055.

SYSTEMS AFFECTED:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 with SP1 for Itanium-based Systems Edition
- Microsoft Windows Server 2003 x64 Edition

RISK:**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High**DESCRIPTION:**

Microsoft has released a patch for a newly discovered vulnerability in Vector Markup Language (VML) implementations on Microsoft Window platforms. This vulnerability exists due to insufficient bounds-checking when handling heap data in the 'vgx.dll' library. Active exploitation of this vulnerability has been reported by Microsoft. If exploited, this vulnerability could allow a remote attacker to execute arbitrary programs on the system in the context of the current user. If user is logged on with the administrator privileges, an attacker could take complete administrative control of the affected system.

This flaw can be exploited by visiting specific malicious web sites with Internet Explorer or by viewing malicious HTML email messages in Outlook.

It should be noted that this vulnerability is not the same vulnerability that was addressed in MS06-055, however this patch (MS07-004) replaces the original patch provided in MS06-055.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the appropriate patch listed in MS07-004 to all vulnerable systems immediately after appropriate testing.
- Ensure that all anti-virus software is up to date with the latest signatures.
- If possible, limit user access to trusted Web sites only. Only browse the Internet as a non-privileged user (one without administrative privilege) to diminish the effects of a successful attack.
- Do not open email attachments from un-trusted sources.
- Do not visit un-trusted websites or follow links provided by unknown or untrusted sources.
- Set email client software to show emails in plain text.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/Bulletin/MS07-004.msp>

<http://msdn.microsoft.com/workshop/author/vml/SHAPE/introduction.asp>

US-CERT:

<http://www.kb.cert.org/vuls/id/122084>

Secunia:

<http://secunia.com/advisories/23677/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0024>