



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

December 11, 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:

2007-026

DATE ISSUED:

December 11, 2007

SUBJECT:

Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution

OVERVIEW:

Four vulnerabilities have been identified in Microsoft Internet Explorer that could allow an attacker to take complete control of an affected system. These vulnerabilities can be exploited if a user visits a specifically crafted web page. Successful exploitation will result in an attacker gaining the same user privileges as the logged on user. If the user is logged in with administrator privileges, the attacker could then install programs, view, change, or delete data, or create new accounts with full privileges.

It should be noted that these vulnerabilities are currently being exploited.

SYSTEMS AFFECTED:

- Microsoft Internet Explorer 5.01 Service Pack 4 on Windows 2000 Service Pack 4
- Microsoft Internet Explorer 6 Service Pack 1 when installed on Windows 2000 Service Pack 4
- Microsoft Internet Explorer 6 for Windows XP Service Pack 2
- Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition and Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition Service Pack 2
- Microsoft Internet Explorer 6 for Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 and Service Pack 2
- Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Internet Explorer 7 for Windows XP Service Pack 2

- Windows Internet Explorer 7 for Windows XP Professional x64 Edition and Microsoft Internet Explorer 7 for Windows XP Professional x64 Edition Service Pack 2
- Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1 and Windows Server 2003 x64 Edition Service Pack 2
- Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems and Windows Internet Explorer 7 Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Internet Explorer 7 for Windows Vista
- Windows Internet Explorer 7 for Windows Vista 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:

Four vulnerabilities have been identified in Microsoft Internet Explorer that could allow a remote attacker to execute arbitrary code on the affected systems.

Three Uninitialized Memory Corruption Vulnerabilities

Microsoft released information on three Internet Explorer vulnerabilities that allows an attacker to execute arbitrary code on affected systems. All of these vulnerabilities are the result of Internet Explorer improperly accessing objects that are either not correctly initialized or have been deleted. This improper access results in corruption of system memory in such a way that an attacker could execute arbitrary code.

One DHTML Object Memory Corruption Vulnerability

Microsoft also released information on a memory corruption vulnerability in the way Internet Explorer handles web page containing certain unexpected HTML objects resulting in corruption of system memory in such a way that an attacker could execute arbitrary code.

All of these vulnerabilities can be exploited by an attacker if a user visits a malicious web site. Successful exploitation could allow an attacker to execute arbitrary code on the system. If the user is logged in with administrator privileges, the attacker could then install programs, view, change, or delete data, or create new accounts with full privileges.

RECOMMENDATIONS:

We recommend that the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

- Logon to your systems as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. Employ the principle of least privilege when ever possible.
- Do not visit unknown or un-trusted Web sites or click on links provided in an email.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms07-069.mspx>

SecurityFocus:

<http://www.securityfocus.com/bid/26427>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3902>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3903>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5344>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5347>