



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

October 14, 2008

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:

2008-019

DATE(S) ISSUED:

10/14/2008

SUBJECT:

Vulnerabilities in Internet Explorer Could Allow Remote Code Execution

OVERVIEW:

Six vulnerabilities have been discovered in Microsoft Internet Explorer that could allow an attacker to take complete control of an affected system. These vulnerabilities may be exploited if a user visits a specifically crafted web page. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. If the user is logged in with administrator privileges, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

- Internet Explorer 5.01
- Internet Explorer 6
- Internet Explorer 7

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:

Six vulnerabilities have been discovered in Microsoft Internet Explorer that could allow an attacker to take complete control of an affected system. Details of these vulnerabilities including the initial Microsoft Exploitability Index Assessment rating are noted below. The Exploitability Index uses one of three values to communicate to customers the likelihood of functioning exploit code, based on vulnerabilities addressed by Microsoft security bulletins. The ratings are as follows: 1- Consistent exploit code likely; 2 - Inconsistent exploit code likely; 3 - Functioning exploit code unlikely.

Window Location Property Cross-Domain Vulnerability – rating - public at bulletin release

HTML Element Cross-Domain Vulnerability – rating - 1

Event Handling Cross-Domain Vulnerability – rating - 1

Three vulnerabilities have been discovered in the way Internet Explorer determines the origin of a script. This can result in a script running in the context of a security zone other than that which it originated.

Successful exploitation of systems running Internet Explorer 5.01 or Internet Explorer 6 on Microsoft Windows 2000 SP4 could allow an attacker to execute arbitrary code on the affected 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.

Successful exploitation of systems running Internet Explorer 6 or Internet Explorer 7 running on Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008 can result in information disclosure.

Cross-Domain Information Disclosure Vulnerability – rating - 3

A vulnerability has been discovered in the way Internet Explorer determines the origin of a script. This can result in a script running in the context of a security zone other than that which it originated.

Successful exploitation could result in information disclosure on all affected systems.

Uninitialized Memory Corruption Vulnerability – rating - 2

HTML Objects Memory Corruption Vulnerability – rating - 3

Two vulnerabilities have been discovered in the way Internet Explorer accesses certain objects in memory. Specifically, Internet Explorer may attempt to access an object which has not properly been initialized or has been deleted.

Successful exploitation could allow an attacker to execute arbitrary code on the affected 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 the following actions be taken:

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

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS08-058.msp>

<http://technet.microsoft.com/en-us/security/cc998259.aspx>

<http://www.microsoft.com/technet/security/bulletin/ms08-oct.msp>

Security Focus:

<http://www.securityfocus.com/bid/31615>

<http://www.securityfocus.com/bid/31618>

<http://www.securityfocus.com/bid/31617>

<http://www.securityfocus.com/bid/31616>

<http://www.securityfocus.com/bid/29960>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2947>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3472>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3473>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3474>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3475>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3476>