



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

August 9, 2011

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.

**ADVISORY NUMBER:
SA2011-043**

**DATE(S) ISSUED:
08/09/2011**

**SUBJECT:
Cumulative Security Update for Internet Explorer (MS11-057)**

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining 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. Several of the vulnerabilities can also lead to information disclosure if successfully exploited.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9

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:

Seven vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

Remote Code Execution Vulnerabilities

Four remote code execution vulnerabilities have been discovered in Internet Explorer. Three of these vulnerabilities are memory corruption vulnerabilities that occur due to the way Internet Explorer accesses objects in memory that have not been properly initialized, deleted, or corrupted due to a race condition. An additional vulnerability could allow an attacker to use Internet Explorer in order to invoke the telnet URI handler in such a way that would allow remote code to run on the user's machine. These vulnerabilities may be exploited if a user visits a web page that is specifically crafted to take advantage of the vulnerabilities. Successful exploitation of any of these vulnerabilities could result in an attacker taking complete control of the system.

Information Disclosure Vulnerabilities

Three information disclosure vulnerabilities have also been discovered in Internet Explorer. An attacker could successfully exploit the first vulnerability by convincing a user to visit a specially crafted website and perform a drag and drop operation on the page. This could allow the attacker to view cookie files stored on the local machine. The second and third vulnerabilities can be exploited by convincing a user to visit a specially crafted website, which would allow an attacker to access information in other domains or Internet Explorer Zones.

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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms11-057.msp>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1257>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1261>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1262>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1260>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1263>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1264>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1283>

SecurityFocus:

<http://www.securityfocus.com/bid/49027>

<http://www.securityfocus.com/bid/49023>

<http://www.securityfocus.com/bid/48994>

<http://www.securityfocus.com/bid/49032>

<http://www.securityfocus.com/bid/49039>

<http://www.securityfocus.com/bid/49037>

<http://www.securityfocus.com/bid/47989>

Sophos:

<http://esp.sophos.com/support/knowledgebase/article/113983.html?rate>