



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

February 12, 2013

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:

SA2013-013

DATE(S) ISSUED:

02/12/2013

SUBJECT:

Cumulative Security Update for Internet Explorer (MS13-009)

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.

SYSTEMS AFFECTED:

- Internet Explorer 10
- Internet Explorer 9
- Internet Explorer 8
- Internet Explorer 7
- Internet Explorer 6

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:

Twelve remote code execution vulnerabilities and one information disclosure vulnerability have been discovered in Internet Explorer. The vulnerabilities that allow remote code execution occur due to the way Internet Explorer accesses objects in memory that have not been properly initialized or deleted. The information disclosure vulnerability occurs due to the way Internet Explorer handles certain types of encoding. These vulnerabilities can be exploited if a user visits a web page that is specifically crafted to take advantage of the vulnerabilities. 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.

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.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. (Macintosh).

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-009>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0015>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0018>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0019>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0020>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0021>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0022>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0023>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0024>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0025>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0026>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0027>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0028>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0029>