State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

April 10, 2012

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:
SA2012-018

DATE(S) ISSUED:
4/10/2012

SUBJECT:
Cumulative Security Update for Internet Explorer (MS12-023)

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 anattacker 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 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:

Five remote code execution vulnerabilities have been discovered in Microsoft Internet Explorer. The first vulnerability is caused by the way Internet Explorer improperly handles printing a specially crafted HTML page. The remaining four vulnerabilities are memory corruption issues that occur whenInternet Explorer attempts to access objects in memory that have already been deleted. These vulnerabilities may be exploited if a user visits a web pagethat 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.

RECOMMENDATIONS:

Werecommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediatelyafter 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://technet.microsoft.com/en-us/security/bulletin/ms12-023

Security Focus:

http://www.securityfocus.com/bid/52889
http://www.securityfocus.com/bid/52904
http://www.securityfocus.com/bid/52902
http://www.securityfocus.com/bid/52905
http://www.securityfocus.com/bid/52906

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0168
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0169
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0170
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0171
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0172