



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

April 28, 2014

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:

SA2014-032

DATE(S) ISSUED:

4/28/2014

05/01/2014 - **Updated**

SUBJECT:

Vulnerability in Internet Explorer Could Allow Remote Code Execution (MS14-021)

EXECUTIVE SUMMARY:

A vulnerability has 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 this vulnerability 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.

UPDATED EXECUTIVE SUMMARY

Microsoft released updates for Internet Explorer versions 6 through 11 on Windows XP and newer workstations, and Windows server 2003 and newer servers. Please note that a security update for XP is available, however, organizations and users are strongly recommended to expedite the migration plans for a newer operating system as Windows XP is end-of-lifed as of April 2013 and will no longer be supported by Microsoft.

THREAT INTELLIGENCE:

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild. Microsoft is reporting targeted attacks that attempt to exploit this vulnerability in Internet Explorer 6 through Internet Explorer 11.

SYSTEMS AFFECTED:

Microsoft Internet Explorer 6

Microsoft Internet Explorer 7

Microsoft Internet Explorer 8

Microsoft Internet Explorer 9

Microsoft Internet Explorer 10
Microsoft Internet Explorer 11

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

TECHNICAL SUMMARY:

A vulnerability has been reported affecting all versions of Internet Explorer that could allow for remote code execution. This vulnerability exists due to the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code, in the context of the current user, within Internet Explorer. An attacker could host a specially crafted website designed to take advantage of this vulnerability, and then convince or trick an unsuspecting user to visit their site.

Successful exploitation of this vulnerability 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:
Consider using an alternate browser until a patch is made available for the vulnerable versions of Internet Explorer.
Consider implementing Microsoft's Enhanced Mitigation Experience Toolkit (EMET) as it has been reported to make the vulnerability difficult to exploit.
Run Internet Explorer with Protected Mode enabled
Set Internet and Local intranet security zone settings to "High"
Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

UPDATED RECOMMENDATIONS

Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
Run Internet Explorer with Enhanced Protected Mode enabled
Consider implementing Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Version 4.0 as it has been reported to make the vulnerability difficult to exploit. Please note that earlier versions of EMET is not effective for this vulnerability.

REFERENCES:

Fireeye:
<http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html>

Microsoft:
<https://technet.microsoft.com/en-US/library/security/2963983>

<http://technet.microsoft.com/en-US/security/jj653751>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776>

UPDATED REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/ms14-021>