



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

December 31, 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:
SA2012-084

DATE(S) ISSUED:
12/29/2012
12/31/2012 – *UPDATED*
01/14/2013 – *UPDATED*

SUBJECT:
Vulnerability in Internet Explorer Could Allow Remote Code Execution

OVERVIEW:
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. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of the vulnerability. 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. Failed exploit attempts may result in a denial-of-service condition.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild resulting in remote code execution.

Please also note that the MS-ISAC received reports that Council on Foreign Relations (CFR) website cfr.org had been compromised and a malicious javascript was inserted into the webpage located at "[hxxp://cfr\[.\]org/js/js/news_123432476.html](http://hxxp://cfr[.]org/js/js/news_123432476.html)". This malicious script was exploiting I.E. Zero day vulnerability discussed in this advisory since December 7, 2012. The CFR is currently aware of the issue and have corrected their website. if the exploitation was successful, compromised system would connect to a subdomain of ".yourtrap.com".

December 31, 2012 UPDATED OVERVIEW:

Microsoft has released a "Fix It" solution that will apply the workarounds in security advisory 2794220.

January 14, 2013 UPDATED OVERVIEW:

Microsoft has released an update for Internet Explorer that fixes this vulnerability ('CDwnBindInfo' Use-After-Free - CVE-2012-4792) in out-of-cycle bulletin MS13-008.

SYSTEMS AFFECTED:

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

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:

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. The 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.

Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of the 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. Failed exploit attempts may result in a denial-of-service condition.

~~**It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild resulting in remote code execution.**~~

Please also note that the MS-ISAC received reports that Council on Foreign Relations (CFR) website cfr.org had been compromised and a malicious javascript was inserted into the webpage located at "hxxp://cfr[.]org/js/js/news_123432476.html". This malicious script was exploiting I.E. Zero day vulnerability discussed in this advisory since December 7, 2012. The CFR is currently aware of the issue and have corrected their website. if the exploitation was successful, compromised system would connect to a subdomain of ".yourtrap.com".

December 31, 2012 UPDATED DESCRIPTION:

Microsoft has released a "Fix It" solution that will apply the workarounds in security advisory 2794220.

January 14, 2013 UPDATED DESCRIPTION:

Microsoft has released an update for Internet Explorer that fixes this vulnerability ('CDwnBindInfo' Use-After-Free - CVE-2012-4792) in out-of-cycle bulletin MS13-008.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade to the most recent version of Internet Explorer immediately after appropriate testing.
- If upgrading Internet Explorer is not feasible, consider using an alternate browser until this vulnerability is remediated.
- 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.
- Review your network logs for traffic to the above network indicators.

December 31, 2012 UPDATED RECOMMENDATIONS:

- Consider implementing the "Fix It" solution provided by Microsoft.

January 14, 2013 UPDATED RECOMMENDATIONS:

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

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/advisory/2794220>

<http://blogs.technet.com/b/srd/archive/2012/12/29/new-vulnerability-affecting-internet-explorer-8-users.aspx>

http://blogs.technet.com/b/msrc/archive/2012/12/29/microsoft-releases-security-advisory-2794220.aspx?utm_source=twitterfeed&utm_medium=twitter

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4792>

NextWeb:

<http://thenextweb.com/microsoft/2012/12/29/criminals-use-adobe-flash-and-new-ie-vulnerability-in-targeted-attacks-ie9-and-ie10-users-are-safe/>

AlienVault:

<http://labs.alienvault.com/labs/index.php/2012/just-another-water-hole-campaign-using-an-internet-explorer-0day/>

December 31, 2012 UPDATED REFERENCES:

Microsoft:

<http://support.microsoft.com/kb/2794220>

January 14, 2013 UPDATED REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-008>

SecurityFocus:

<http://www.securityfocus.com/bid/57070>