

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

February 8, 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:

SA2010-094

DATE(S) ISSUED:

12/21/2010

2/8/2011 - Updated

SUBJECT:

Vulnerability in Internet Explorer Could Allow Remote Code Execution

ORIGINAL OVERVIEW:

A new 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 a working exploit is available which results in remote code execution. The exploit has been tested by the MS-ISAC with Internet Explorer 7 & 8 on a Windows XP SP3 platform and confirmed to result in remote code execution.**~~

UPDATED OVERVIEW:

A patch has been made available for this vulnerability in Microsoft Bulletin MS11-003.

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**ORIGINAL DESCRIPTION:**

A new 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 occurs when rendering a web page containing a reference to a Cascading Style Sheet (CSS) file with "@import" rules. This may result in a use-after-free condition in the mshtml.dll library. A use-after-free condition occurs when an application deallocates a memory block and then later attempts to access that deallocated space.

Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of these vulnerabilities. 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 a working exploit is available which results in remote code execution. The exploit has been tested by the MS-ISAC with Internet Explorer 7 & 8 on a Windows XP SP3 platform and confirmed to result in remote code execution.

UPDATED DESCRIPTION:

A patch has been made available for this vulnerability in Microsoft Bulletin MS11-003.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions be taken:

- Set Internet and Local Intranet security zone settings to block ActiveX controls and Active Scripting.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Read email in plain-text format.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- If you have an alternate browser deployed, consider using it until this vulnerability is remediated.

UPDATED RECOMMENDATIONS:

We recommend the following actions be taken:

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

ORIGINAL REFERENCES:**US-CERT:**

<http://www.kb.cert.org/vuls/id/634956>

Secunia:

<http://secunia.com/advisories/42510>

Threat Post:

http://threatpost.com/en_us/blogs/new-remotely-exploitable-bug-found-internet-explorer-121010

Full Disclosure:

<http://seclists.org/fulldisclosure/2010/Dec/110>

Metasploit:

https://www.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/ms11_xxx_ie_css_import.rb

UPDATED REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS11-006.mspx>

<http://www.microsoft.com/technet/security/advisory/2490606.mspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3970>