

State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

February 17, 2010

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:

SA2010-015

DATE(S) ISSUED:

3/1/2010

3/2/2010 - UPDATED

4/13/2010 - UPDATED

SUBJECT:

Vulnerability in Internet Explorer Could Allow Remote Code Execution

ORIGINAL 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. **At this point in time, no patches are available for this vulnerability.** Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. 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.

Please note: Proof of concept code has been published and is publically available. However, we have not received any reports of active exploitation of this vulnerability.

March 2 - UPDATED OVERVIEW:

Based on additional testing performed in our lab, we have determined that Windows Server 2008 and Windows Vista are not affected by this vulnerability.

April 13 - UPDATED OVERVIEW:

Microsoft Security Bulletin MS10-022 has been released with a patch for this vulnerability. Please note that this vulnerability was originally listed for Internet Explorer. However, Microsoft has determined that the vulnerability is in the VBScript Scripting Engine. VBScript (Visual Basic Script) is a programming language that is often used to make Web sites more flexible or interactive. Even though Windows Server 2008, Windows 7 and Windows Vista are not exploitable by this vulnerability, the patch should still be applied to these systems.

ORIGINAL SYSTEMS AFFECTED:

- Windows XP
- Windows 2000

- Windows Sever 2003
- ~~Windows Server 2008~~
- ~~Windows Vista~~
- Windows NT
- ~~Microsoft Internet Explorer 6~~
- ~~Microsoft Internet Explorer 7~~
- ~~Microsoft Internet Explorer 8~~

April 13 - UPDATE SYSTEMS AFFECTED:

- Windows Vista
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

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 vulnerability has been identified in Microsoft Internet Explorer that could allow an attacker to take complete control of an affected system. The is due to a vulnerability in the VBScript "MsgBox()" function allowing the execution of malicious Microsoft HELP (.hlp) files by winhlp32.exe. An attacker can exploit this vulnerability by hosting a specially crafted webpage. Once the user visits the page, a specially crafted popup box will then prompt the user to press the "F1" Help key. When the user invokes the Windows help command by pressing the "F1" key, the attacker's code will run inside the browser and exploit the vulnerability.

Successful exploitation could allow an attacker to gain 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. ~~At this point in time, no patches are available for this vulnerability.~~

Please note: Proof of concept code has been published and is publically available. Based on testing in our lab, the PoC code depends on .hlp files being hosted on an SMB share on the Internet. However, this may not be the only attack vector. The PoC code can easily be modified to execute any arbitrary command.

April 13 - UPDATED DESCRIPTION:

Microsoft Security Bulletin MS10-022 has been released with a patch for this vulnerability. Please note that this vulnerability was originally listed for Internet Explorer. However, Microsoft has determined that the vulnerability is in the

VBScript Scripting Engine. VBScript (Visual Basic Script) is a programming language that is often used to make Web sites more flexible or interactive. Even though Windows Server 2008, Windows 7 and Windows Vista are not exploitable by this vulnerability, the patch should still be applied to these systems.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Implement egress and ingress filtering for TCP ports 139 and 445 at your network perimeter.
- Ensure that all Microsoft Internet Explorer clients are configured to prompt before executing Active Scripting. If Active Scripting is not required it should be disabled completely.
- If your organization has deployed alternate browsers, recommend staff utilize an alternate browser.
- If you believe you have been affected by attacks exploiting this vulnerability, please contact us immediately.

April 13 - UPDATED RECOMMENDATIONS:

We recommend the following actions be taken:

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

ORIGINAL REFERENCES:

Microsoft:

<http://blogs.technet.com/msrc/archive/2010/02/28/investigating-a-new-win32hlp-and-internet-explorer-issue.aspx>

Security Focus:

<http://www.securityfocus.com/bid/38463>

Secunia:

<http://secunia.com/advisories/38727>

Vupen:

<http://www.vupen.com/english/advisories/2010/0485>

March 2 - UPDATED REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/981169.mspx>

April 13 - UPDATED REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS10-022.mspx>

<http://www.microsoft.com/technet/security/advisory/981169.mspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0483>

USCERT:

<http://www.kb.cert.org/vuls/id/612021>

Security Focus:

<http://www.securityfocus.com/bid/38463>