

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

August 11, 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:

SA2010-059

DATE(S) ISSUED:

8/11/2010

SUBJECT:

Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS10-053)

OVERVIEW:

Six vulnerabilities have 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 these vulnerabilities. Successful exploitation of these vulnerabilities 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.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Windows XP SP3
- Windows Server 2003
- Windows Server 2008
- Windows Vista
- Windows 7

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:**

Six vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

Event Handler Cross-Domain Vulnerability

An information disclosure vulnerability exists in Microsoft Internet Explorer that could allow a remote attacker access to sensitive data. More specifically, a script could be written that would allow the attacker to gain access in another domain or Internet Explorer zone. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker viewing content from the local computer or another browser window in another domain or Internet Explorer zone.

Three Uninitialized Memory Corruption Vulnerabilities

Three remote code execution vulnerabilities exist in the way that Microsoft Internet Explorer accesses an object that has not been correctly initialized or deleted. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. When a user views the Web page, the vulnerability could allow remote code execution. Successfully exploiting this issue will give the attacker access in the context of the currently 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.

Race Condition Memory Corruption Vulnerability

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that may have been corrupted due to a race condition. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this 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.

HTML Layout Memory Corruption Vulnerability

A remote code execution vulnerability has been discovered in the way that Internet Explorer accesses an object that has not been correctly initialized or deleted. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. When a user views the Web page, the vulnerability could allow remote code execution. Successfully exploiting this issue may give the attacker access in the context of the currently 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.

It should be noted that, by default, Internet Explorer on Windows Server 2003 and Windows Server 2008 runs in a restricted mode that is known as Enhanced Security Configuration. Enhanced Security Configuration is a group of preconfigured settings in Internet Explorer that can reduce the likelihood of a user or administrator downloading and running specially crafted Web content on a server. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to the Internet Explorer Trusted sites zone.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider configuring Internet Explorer to prompt before running Active Scripting or to disable Active Scripting.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS10-053.msp>

Security Focus:

<http://www.securityfocus.com/bid/42288>

<http://www.securityfocus.com/bid/42289>

<http://www.securityfocus.com/bid/42257>

<http://www.securityfocus.com/bid/42292>

<http://www.securityfocus.com/bid/42290>

<http://www.securityfocus.com/bid/42258>

Secunia:

<http://secunia.com/advisories/40895/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1258>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2556>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2557>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2558>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2559>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2560>