

# State of Alaska State Security Office



## Cyber Security Advisory

October 24, 2007

*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.*

### STATE OF ALASKA ADVISORY NUMBER:

2007-022

### DATE ISSUED:

October 24, 2007

### SUBJECT:

New Vulnerability in Windows URI Handler Could Allow for Remote Code Execution

### OVERVIEW:

A new vulnerability has been discovered in the way that Internet Explorer interacts with other software products that could allow arbitrary remote code execution on a fully patched Windows XP or Vista system. This vulnerability can be exploited if a user visits a malicious web page or opens a PDF document which is specifically crafted to exploit this vulnerability.

It should be noted that this vulnerability can be exploited through any affected legitimate application on systems where IE 7.0 is installed. We are currently aware of publicly available exploit code. There has also been limited exploitation of this vulnerability through Adobe Acrobat 8.1 and earlier.

Although some recommendations are provided below to minimize risk, please note that Adobe has released a patch which prevents this vulnerability from being exploited in Adobe Acrobat Reader. See references for patch download locations and additional information. We

recommend that this patch be installed immediately on all affected systems after appropriate testing.

#### **SYSTEMS AFFECTED:**

- Microsoft Windows XP Media Service Pack 2
- Microsoft Windows XP Professional
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows XP Home
- Microsoft Windows Vista Home, Business, Enterprise

#### **APPLICATIONS AFFECTED:**

- Microsoft Internet Explorer 7.0 and at least one of the following:
- Mozilla Firefox 2.0.6 and earlier
- Netscape Navigator 7.1
- Adobe Acrobat Reader 8.1 and earlier
- Adobe Acrobat Standard, Pro and Elements 8.1
- Adobe Acrobat 3D
- Skype in versions prior to 3.5.0.239
- Miranda 0.7
- mIRC
- Possibly other applications

#### **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:**

Microsoft Windows fails to properly handle protocols specified in a Uniform Resource Identifier (URI), which could allow arbitrary remote code execution on a vulnerable system. The URI is a string of characters that can be used to identify a location, resource or protocol. Microsoft Windows will utilize a URI to determine the appropriate application that is registered to handle the protocol. Examples of URI registered handlers include "mailto", "telnet", and "news". The

targeted user must have an application installed which accepts command line options after the URI passed to the protocol handler.

This vulnerability can be exploited if a user visits a malicious web page, opens a malicious email, or opens a PDF document which is specifically crafted to exploit this vulnerability. Upon successful exploitation, the attacker could run arbitrary code in the context of the locally logged-in user. This could also allow the attacker to install programs; add, view or delete user data; or create new accounts on the systems.

***Please note that publicly available exploit code will only execute on systems where Internet Explorer version 7.0 and another vulnerable application are installed. If either of these conditions is not met, the host system is not vulnerable. However, if these conditions are met, the desired exploit code will execute with the assigned URI handler registered to the vulnerable system.***

Microsoft has acknowledged, but has not released a patch to address this vulnerability at this time.

## **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not open email attachments, including PDFs, from untrusted sources.
- Do not visit unknown or un-trusted Web sites or click on links provided in an email.
- Apply the appropriate Adobe Acrobat Reader patch to vulnerable systems immediately after appropriate testing. The patch is available at:

<http://www.adobe.com/support/security/bulletins/apsb07-18.html>

## **REFERENCES:**

### **Microsoft:**

<http://www.microsoft.com/technet/security/advisory/943521.mspx>

<http://support.microsoft.com/kb/224816>

### **Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb07-18.html>

### **US CERT:**

<http://www.kb.cert.org/vuls/id/403150>

<http://www.kb.cert.org/vuls/id/783400>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3896>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3924>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5020>

**Secunia:**

<http://secunia.com/advisories/26201/>

**Security Focus:**

<http://www.securityfocus.com/bid/25945>

<http://www.securityfocus.com/bid/25748>