

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

DATE(S) ISSUED:

6/8/2010

SUBJECT:

Cumulative Security Update of ActiveX Kill Bits (MS10-034)

OVERVIEW:

Microsoft has released a security update which addresses vulnerabilities discovered in multiple ActiveX controls. ActiveX controls are small programs or animations that are downloaded or embedded in web pages which will typically enhance functionality and user experience. Many web design and development tools have built ActiveX support into their products, allowing developers to both create and make use of ActiveX controls in their programs. There are more than 1,000 existing ActiveX controls available for use today.

When vulnerabilities are discovered in ActiveX controls, attackers may use specially crafted web pages to exploit these vulnerabilities. Successful exploitation will result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user, an attacker could then install programs; view, change, or delete data; or create new accounts.

SYSTEMS AFFECTED:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- 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:

Microsoft Internet Explorer includes a security feature which will prevent an ActiveX control from being loaded by using registry settings. This is commonly referred to as setting the 'kill bit' of an ActiveX component. Once the kill bit is set, the associated component can never be loaded.

These vulnerabilities could allow an attacker to take complete control of an affected system, and could be exploited if a user visits a specifically crafted web page.

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.

This update will set the kill bits for the following Class Identifier (CLSID):

Office Excel ActiveX control for Data Analysis (max3activex.dll)

CLSID - 14FD1463-1F3F-4357-9C03-2080B442F503

CLSID - E9CB13DB-20AB-43C5-B283-977C58FB5754

This vulnerability for the Microsoft Data Analyzer ActiveX control is not installed by default and requires manual installation by a user.

Microsoft Internet Explorer 8 Developer Tools (iedvtool.dll)

CLSID - 8fe85d00-4647-40b9-87e4-5eb8a52f4759

Microsoft Internet Explorer 8 Developer Tools are installed and enabled by default for Internet Explorer 8. This vulnerability does not affect hosts running Internet Explorer 6 or Internet Explorer 7 that have Developer tools installed on them.

Additionally, this update will set the Class Identifier (CLSID) for the following third party software:

Danske eSec ActiveX control

CLSID - F6A56D95-A3A3-11D2-AC26-400000058481

PSFormX ActiveX control

CLSID - 56393399-041A-4650-94C7-13DFCB1F4665

Ofoto Upload Manager / Kodak Gallery Easy Upload Manager ActiveX Control

CLSID - 6f750200-1362-4815-a476-88533de61d0c

CLSID - 6f750201-1362-4815-a476-88533de61d0c

CallPilot Unified Messaging ActiveX Control

CLSID - 7F14A9EE-6989-11D5-8152-00C04F191FCA

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate update provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Configure Internet Explorer to prompt before running ActiveX Controls or disable ActiveX controls in the Internet Zone.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/Ms10-034.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0252>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0811>