



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

September 8, 2009

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:

SA2009-053

SUBJECT:

Vulnerability in Microsoft DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (MS09-046)

OVERVIEW:

A vulnerability exists in Dynamic Hyper Text Markup Language (DHTML) Editing Component which may allow an attacker to take complete control of a system. DHTML allows for dynamic content to provide interactive web pages. This vulnerability can be exploited if a user visits a specially crafted web page designed to exploit this vulnerability. Successful exploitation 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:

- Windows 2000
- Windows XP
- Windows Server 2003

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:

A vulnerability exists in Dynamic Hyper Text Markup Language (DHTML) which may allow an attacker to take complete control of a system. The DHTML Document Object Model (DOM) allows authors direct, programmable access to individual components of their Web documents. This access, combined with the DOM model, allows the browser to react to user input and execute scripts. This vulnerability can be exploited if a user visits a specially crafted web page designed to exploit this vulnerability. Successful exploitation 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.

On Windows Server 2003, Internet Explorer runs in restricted mode by default. In this mode, the Internet zone is set to high which will prompt the user before running ActiveX controls. However, websites that have been added as trusted sites will not prompt the user before running ActiveX controls.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the appropriate patch 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.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Set the kill bit on the Class Identifier (CLSID) {2D360201-FFFS-11D1-8D03-00A0C959BC0A}; further instructions on how to set the kill bit can be found at the following location (<http://support.microsoft.com/kb/240797>).

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS09-046.mspx>
<http://support.microsoft.com/kb/240797>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2519>

Security Focus:

<http://www.securityfocus.com/bid/36280>