

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

January 11, 2011

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:

SA2011-002

DATE(S) ISSUED:

1/11/2011

SUBJECT:

Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (MS11-002)

OVERVIEW:

Two vulnerabilities have been discovered in Microsoft Data Access Components, which could allow an attacker to take complete control of an affected system. Microsoft Data Access Components (MDAC) is a collection of applications that make it easy for programs to access databases. 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. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

- 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:

Two vulnerabilities have been discovered in Microsoft Data Access Components, which could allow an attacker to take complete control of an affected system. The first vulnerability is a buffer overflow in the Data Source Name (DSN) argument of an Open Database Connectivity (ODBC) API. This vulnerability cannot be leveraged remotely unless a third party application is used to access ODBC APIs. An attacker can exploit this issue by convincing a user to visit a specially crafted web page designed to cause a buffer overflow with a specially crafted DSN. This will allow the attacker to execute arbitrary code in the context of the logged-on user.

The second vulnerability is due to the way MDAC validates memory allocation. In a web-based attack scenario, exploitation may occur if a user visits a specially crafted website designed to exploit this issue. 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. Failed exploit attempts may result in a denial-of-service condition.

It should be noted that, by default, Internet Explorer on Windows Server 2003 and Windows Server 2008 runs in a restricted mode 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. Also, all supported versions of Microsoft Outlook, Outlook Express, and Windows Mail open HTML e-mail messages in the restricted sites zone, which disables script and ActiveX controls which removes the risk of an attacker being able to execute malicious code within an e-mail.

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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails especially from untrusted sources.
- Remind users not to download or open files from untrusted websites.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS11-002.mspx>

<http://blogs.technet.com/b/msrc/archive/2011/01/10/january-2011-security-bulletins.aspx>

<http://support.microsoft.com/kb/2451910>

SANS:

<https://isc.sans.edu/diary.html?storyid=10252>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0026>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0027>