



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

April 13, 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:

SA2011-023

DATE(S) ISSUED:

4/13/2011

SUBJECT:

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS11-023)

OVERVIEW:

Multiple vulnerabilities have been identified in Microsoft Office, which is Microsoft's business application suite. These vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file or a legitimate Microsoft Office file that located in the same network directory as a malicious library file. 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:

- Microsoft Office XP
- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2004 for Mac
- Microsoft Office 2008 for Mac
- Open XML File Format Converter for Mac

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 identified in Microsoft Office that could allow an attacker to take complete control of an affected system. Details of these vulnerabilities are as follows:

Office Component Insecure Library Loading Vulnerability

The vulnerability is caused when Microsoft Office incorrectly restricts the path used for loading external libraries. This can be exploited by a user opening a legitimate Office-related file (such as a .docx file) that is located in the same network directory as a specially crafted dynamic link library (DLL) file. Microsoft Office could then attempt to load the DLL file and execute any code it contained. This vulnerability has been publicly disclosed.

Microsoft Office Graphic Object Dereferencing Vulnerability

The vulnerability is caused when Microsoft Office does not properly handle dereferencing data structures when parsing a specially crafted Office file that contains graphic objects. This vulnerability can be triggered by opening a specially crafted Microsoft Office file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted Microsoft Office file as an email attachment. In the web based scenario, a user would have to open the specially crafted Microsoft Office file that is hosted on a website. When the user opens the Microsoft Office file, the attacker's supplied code will execute.

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.

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.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Remind users not to open email attachments from unknown or untrusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS11-023.msp>
<http://support.microsoft.com/kb/2505927>
<http://support.microsoft.com/kb/2509461>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0107>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0977>

VUPEN:

<http://www.vupen.com/english/advisories/2011/0942>

SecurityFocus:

? <http://www.securityfocus.com/bid/47246>
? <http://www.securityfocus.com/bid/46227>