

# State of Alaska State Security Office



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

November 9, 2010

*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:**

SA2010-085

**DATE(S) ISSUED:**

11/9/2010

**SUBJECT:**

Multiple Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS10-087)

**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 Office file, Rich Text Format (RTF) file or malicious Dynamic Link Library (DLL) file and can be exploited via email or through the web.

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:**

- Microsoft Office XP
- Microsoft Office 2003

- Microsoft Office 2004 for Mac
- Microsoft Office 2007
- Microsoft Office 2008 for Mac
- Microsoft Office 2010
- Microsoft Office 2011 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:**

Multiple 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:

The first vulnerability exists because Microsoft Office fails to perform adequate boundary-checks on user-supplied data. Specifically, this issue occurs when the software parses a specially crafted Rich Text Format (RTF) file.

The second vulnerability is due to the application searching for the 'pptimconv.dll' Dynamic Link Library file in the current working directory. The issue can be exploited by placing a specially crafted library file in an attacker-controlled location along with a file that is associated with the vulnerable application. Using the application to open the associated file will cause the malicious library file to be executed.

The third vulnerability exists because the application fails to properly handle drawing exceptions. This issue can be exploited if a user opens a specially crafted Office file.

The fourth vulnerability affects the Art Drawing record when handling a specially crafted Office file.

The fifth vulnerability exists in Microsoft office when handling a specially crafted Office 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. Failed attempts will result in a denial-of-service.

All but one of these vulnerabilities can be exploited by opening a specially crafted Office file received as an email attachment, or by visiting a web site that is hosting a specially crafted Office file. The DLL vulnerability could be exploited if a user were to first save the specially crafted file in the same directory as an Office file and then be convinced to open the Office file. The DLL vulnerability could also be exploited if a user were to access an attacker controlled location with a vulnerable application.

**It should be noted that there is currently no patch available for Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, and Open XML File Format Converter for Mac.**

#### **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

#### **REFERENCES:**

##### **Microsoft:**

<http://www.microsoft.com/technet/security/Bulletin/MS10-087.mspx>

**Security Focus:**

<http://www.securityfocus.com/bid/42628>

<http://www.securityfocus.com/bid/44652>

<http://www.securityfocus.com/bid/44656>

<http://www.securityfocus.com/bid/44659>

<http://www.securityfocus.com/bid/44660>

**Secunia:**

<http://secunia.com/advisories/40820/>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3334>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3335>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3336>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3337>