

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

June 8, 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:

SA2010-041

DATE(S) ISSUED:

6/8/2010

SUBJECT:

Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (MS10-038)

OVERVIEW:

Multiple vulnerabilities have been identified in Microsoft Office Excel, a spreadsheet application. These vulnerabilities could allow remote code execution if a user opens a specially crafted Excel file. The file may be received as an email attachment, or downloaded via 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
- 2007 Microsoft Office System
- Microsoft Office for Mac
- Microsoft Office 2004 for Mac
- Microsoft Office 2008 for Mac
- Open XML File Format Converter for Mac
- Microsoft Office Excel Viewer
- Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats

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:

Fourteen vulnerabilities have been identified in Microsoft Office Excel that could allow an attacker to take complete control of an affected system. These vulnerabilities can be triggered by opening a specially crafted Excel file (.XLS) and can be exploited via email or through the web. In the email based scenario, the user would have to open the specially crafted Excel file as an email attachment. In the web based scenario, a user would have to open the specially crafted Excel file that is hosted on a website. When the user opens the Excel file, the attacker's supplied code will execute.

Thirteen of these vulnerabilities exist because of the way Microsoft Office Excel parses the Excel file format when processing Excel files. The last vulnerability exists due to the incorrect ACLs being applied to the "/Application" folder on MAC OS X systems. Successful exploitation of any 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 open email attachments from unknown or un-trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Consider using the Microsoft Office Isolated Conversion Environment (MOICE - <http://support.microsoft.com/kb/935865>) to mitigate some of the vulnerabilities identified in this advisory.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms10-038.msp>

<http://support.microsoft.com/kb/935865>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0821>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0822>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0823>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0824>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1245>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1246>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1247>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1248>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1249>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1250>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1251>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1252>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1253>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1254>

Security Focus:

<http://www.securityfocus.com/bid/40518>
<http://www.securityfocus.com/bid/40520>
<http://www.securityfocus.com/bid/40521>
<http://www.securityfocus.com/bid/40522>
<http://www.securityfocus.com/bid/40523>
<http://www.securityfocus.com/bid/40524>
<http://www.securityfocus.com/bid/40525>
<http://www.securityfocus.com/bid/40526>
<http://www.securityfocus.com/bid/40527>
<http://www.securityfocus.com/bid/40528>
<http://www.securityfocus.com/bid/40529>
<http://www.securityfocus.com/bid/40530>
<http://www.securityfocus.com/bid/40531>