

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

October 12, 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:

SA2010-074

DATE (S) ISSUED:

10/12/2010

SUBJECT:

Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (MS10-079)

OVERVIEW:

Eleven vulnerabilities have been discovered in Microsoft Office Word. These vulnerabilities can be exploited by opening a malicious Word document received as an email attachment, or by visiting a website that is hosting a malicious Word document. 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. Failed exploitation could result in denial-of-service conditions.

SYSTEMS AFFECTED:

- Microsoft Office XP
- Microsoft Office 2003

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2004 for Mac
- Microsoft Office 2008 for Mac
- Open XML File Format Converter for Mac
- Microsoft Word Viewer
- Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats
- Microsoft Office Web Apps

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:

Eleven vulnerabilities have been discovered in Microsoft Office Word. Details of these vulnerabilities are as follows:

Word Uninitialized Pointer Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles an uninitialized pointer when parsing a specially crafted Word file. When Microsoft Word parses a specially crafted Word file, system memory may become corrupted in such a way that an attacker could execute arbitrary code

Word Boundary Check Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles an

improper boundary check when parsing a specially crafted Word file. When Microsoft Word parses a specially crafted Word file, an improper boundary check may cause system memory to become corrupted in such a way that an attacker could execute arbitrary code.

Word Index Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles index values inside a specially crafted Word file. When Microsoft Word parses a specially crafted Word file that contains a malformed index value, system memory may become corrupted in such a way that an attacker could execute arbitrary code.

Word Stack Overflow Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles stack validation when parsing a specially crafted Word file. When Microsoft Word parses a specially crafted Word file, system memory may become corrupted in such a way that an attacker could execute arbitrary code.

Word Return Value Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles return values when parsing a specially crafted Word file. When Microsoft Word parses a specially crafted Word file, system memory may become corrupted in such a way that an attacker could execute arbitrary code.

Word Bookmarks Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles bookmarks when parsing a specially crafted Word file. When Microsoft Word parses a specially crafted Word file that contains bookmarks, system memory may become corrupted in such a way that an attacker could execute arbitrary code.

Word Pointer Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles pointers when parsing a specially crafted Word file. When Microsoft Word parses a specially crafted Word file, system memory may become corrupted in such a way that an attacker could execute arbitrary code.

Word Heap Overflow Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles

malformed records inside a specially crafted Word file. When Microsoft Word parses a specially crafted Word file, system memory may become corrupted in such a way that an attacker could execute arbitrary code.

Word Index Parsing Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Word handles indexes when parsing a specially crafted Word file. When Microsoft Word parses a specially crafted Word file, system memory may become corrupted in such a way that an attacker could execute arbitrary code.

Two Word Parsing Vulnerabilities

Two remote code execution vulnerabilities exist in the way that Microsoft Word parses a specially crafted Word file. When Microsoft Word parses a specially crafted Word file, system memory may be corrupted in such a way that an attacker could execute arbitrary code.

Successful exploitation of these vulnerabilities will 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 exploitation could result in denial-of-service conditions.

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 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.
- 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>).

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms10-079.msp>

Security Focus:

<http://www.securityfocus.com/bid/43754>

<http://www.securityfocus.com/bid/43760>

<http://www.securityfocus.com/bid/43765>

<http://www.securityfocus.com/bid/43766>

<http://www.securityfocus.com/bid/43767>

<http://www.securityfocus.com/bid/43769>

<http://www.securityfocus.com/bid/43770>

<http://www.securityfocus.com/bid/43771>

<http://www.securityfocus.com/bid/43782>

<http://www.securityfocus.com/bid/43783>

<http://www.securityfocus.com/bid/43784>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2747>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2748>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2750>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3214>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3215>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3216>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3217>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3218>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3219>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3220>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3221>