

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

August 10, 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:

SA2010-055

DATE(S) ISSUED:

8/10/2010

SUBJECT:

Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (MS10-056)

OVERVIEW:

Four 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 web site 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
- 2007 Microsoft Office System
- Microsoft Office 2004 for Mac
- Microsoft Office 2008 for Mac
- Open XML File Format Converter for Mac
- Microsoft Office Word Viewer
- Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats
- Microsoft Works 9

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:

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

Word Record Parsing Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Office Word handles malformed records inside a specially crafted Word file. When Microsoft Office Word opens a specially crafted Word file, it may corrupt system memory in such a way that an attacker could execute arbitrary code.

Word RTF Parsing Engine Memory Corruption Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Office Word parses rich text data. Microsoft Office Word does not perform sufficient data validation when handling rich text data. When Word opens and parses a specially crafted rich text format (RTF) e-mail message or file, it may corrupt memory in such a way that an attacker could execute arbitrary code.

Word RTF Parsing Buffer Overflow Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Office Word parses certain rich text data. Microsoft Office Word does not perform sufficient data validation when handling rich text data. When Word opens and parses a specially crafted rich text format (RTF) e-mail message or file, it may corrupt memory in such a way that an attacker could execute arbitrary code.

Word HTML Linked Objects Memory Corruption Vulnerability

A remote code execution vulnerability exists in the way that Microsoft Office Word handles a specially crafted Word file that includes a malformed record. When Microsoft Office Word opens a specially crafted Word file, it may corrupt system memory 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/MS10-056.mspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1900>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1901>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1902>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1903>