



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

**December 11, 2012**

*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:**

SA2012-079

**DATE(S) ISSUED:**

12/11/2012

**SUBJECT:**

Vulnerability in Microsoft Word Could Allow Remote Code Execution (MS12-079)

**OVERVIEW:**

A vulnerability has been discovered in Microsoft Office Word that 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 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Word Viewer
- Microsoft Office Compatibility Pack
- Microsoft SharePoint Server 2010
- Microsoft Office Web Apps 2010

**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:**

A remote code execution vulnerability exists in the way that Microsoft Office software parses specially crafted Rich Text Format (RTF) data. This vulnerability can be exploited when a user opens a specially crafted RTF file, or when a user opens or previews a specially crafted RTF email message. The specially crafted RTF file can be sent as an email attachment, or hosted on a website.

Successful exploitation of this vulnerability could allow the attacker to take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative 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.
- Consider viewing emails in plain text.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

**REFERENCES:****Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-079>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2539>

**SecurityFocus:**

<http://www.securityfocus.com/bid/56834>