



State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory

February 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:**

SA2010-010

**DATE(S) ISSUED:**

2/9/2010

**SUBJECT:**

Vulnerability in Microsoft Office Could Allow Remote Code Execution (MS10-003)

**OVERVIEW:**

A vulnerability has been discovered in Microsoft Office which could allow an attacker to take complete control of an affected system. The vulnerability 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. Successful exploitation could allow an attacker to gain 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 2004 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:**

A vulnerability has been identified in Microsoft Office that could allow remote code execution. This vulnerability can be triggered by opening a specially crafted Office file which may cause a buffer-overflow condition. This vulnerability can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted Office file as an email attachment. In the Web based scenario, a user would visit a website and then open the specially crafted Office file that is hosted on the page.

Successful exploitation could allow an attacker to gain 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.
- Remind users not to download or open files from un-trusted websites.

### **REFERENCES:**

#### **Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/ms10-003.mspx>

#### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0243>

#### **SecurityFocus:**

<http://www.securityfocus.com/bid/38073/>