



# State of Alaska State Security Office

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

February 10, 2015

*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:

SA2015-013

### DATE(S) ISSUED:

02/10/2015

### SUBJECT:

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS15-012)

### EXECUTIVE SUMMARY:

This security update resolves three privately reported vulnerabilities in Microsoft Office. These vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user.

### THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Microsoft Excel 2007
- Microsoft Word 2007
- Microsoft Office 2010
- Microsoft Word 2010
- Microsoft Web Applications 2010
- Microsoft Excel 2013
- Microsoft Word Viewer
- Microsoft Excel Viewer
- Microsoft Office Compatibility Pack

**RISK:****Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Home users: High****TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Microsoft Office, specifically in how Microsoft Excel and Microsoft Word parse specially crafted files. This update addresses three remote code execution vulnerabilities including:

- Excel Remote Code Execution Vulnerability (CVE-2015-0063)
- Office Remote Code Execution Vulnerability (CVE-2015-0064)
- OneTableDocumentStream Remote Code Execution Vulnerability (CVE-2015-0065)

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights 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. 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.
- 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:**

<https://technet.microsoft.com/en-us/library/security/MS15-012>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0063>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0064>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0065>