

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

03/10/2015

SUBJECT:

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS15-022)

OVERVIEW:

This security update resolves five 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 the vulnerabilities could run arbitrary code in the context of the current user and take actions on the behalf of the logged-on user with the same permissions as the current user.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Office 2013 RT
- Microsoft Word Viewer
- Microsoft Excel Viewer
- Microsoft Office Compatibility Pack Service Pack 3
- Microsoft SharePoint Server 2007
- Microsoft SharePoint Server 2010
- Microsoft SharePoint Server 2013
- Microsoft Office Web Apps 2010
- Microsoft Office Web Apps 2013

RISK:

Government:

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

Businesses:

- Large and medium businesses: **High**
- Small businesses: **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 five remote code execution vulnerabilities including.

- Microsoft Office Component Use After Free Vulnerability (CVE-2015-0085)
- Microsoft Office Memory Corruption Vulnerability (CVE-2015-0086)
- Microsoft Word Local Zone Remote Code Execution Vulnerability (CVE-2015-0097)
- Microsoft SharePoint XSS Vulnerabilities (CVE-2015-1633; CVE-2015-1636)

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:

The following actions should 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/MS15-022>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0085>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0086>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0097>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1633>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1636>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>