

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:

10/13/2015

SUBJECT:

Security Updates for Microsoft Office to Address Remote Code Execution (MS15-110)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office. The most severe of these vulnerabilities could allow remote code execution. Successful exploitation of these vulnerabilities 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.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- Microsoft Excel 2007
- Microsoft Excel 2010
- Microsoft Excel for Mac 2011
- Microsoft Excel 2013
- Microsoft Excel 2013 RT
- Microsoft Excel 2016
- Microsoft Excel 2016 for Mac
- Microsoft Excel Viewer
- Microsoft Visio 2007
- Microsoft Visio 2010
- Microsoft Office Compatibility Pack
- Microsoft Excel Web App 2010
- Microsoft Web App 2010
- Microsoft Office Web Apps Server 2013
- Microsoft SharePoint Server 2007
- Excel Services on Microsoft SharePoint Server 2007
- Microsoft SharePoint Server 2010
- Excel Services on Microsoft SharePoint Server 2010
- Microsoft SharePoint Server 2013
- Excel Services on Microsoft SharePoint Server 2013
- Microsoft SharePoint Foundation 2013

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: Low

TECHNICAL SUMMARY:

Six vulnerabilities have been discovered in Microsoft Office. The most severe of these vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file and can be exploited via email or web. An attacker who successfully exploited these vulnerabilities could run arbitrary code in the context of the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Details of these vulnerabilities are as follows:

- Three memory corruption vulnerabilities exist in the way Office handles objects in memory (CVE-2015-2555; CVE-2015-2557; CVE-2015-2558)
- One Microsoft Information Disclosure Vulnerability (CVE-2015-2556)
- One Microsoft Office Web Apps XSS Spoofing Vulnerability (CVE-2015-6037)
- One Microsoft SharePoint Security Feature Bypass Vulnerability (CVE-2015-6039)

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 visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Unless there is a business need to do otherwise, consider disabling XBAPs in Internet Explorer 6, 7, 8. By default, newer versions of Internet Explorer no longer allow XBAPs to run on Internet websites, but they still function in the Local Intranet and Trusted Zones.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/MS15-110>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2555>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2556>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2557>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2558>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6037>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6039>

TLP: WHITE

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

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