

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:

07/12/2016

SUBJECT:

Multiple Vulnerabilities in Microsoft Office Could Allow for Remote Code Execution (MS16-088)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office, the most severe of which could allow for remote code execution if a user opens a specially crafted Microsoft Office file. 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. 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.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- Microsoft Office 2007, 2010, 2013, 2013 RT, 2016
- Microsoft Office for Mac 2011
- Microsoft Office 2016 for Mac
- Microsoft Office Compatibility Pack Service Pack 3
- Microsoft Excel Viewer
- Microsoft Word Viewer
- Microsoft SharePoint Server 2010, 2013, 2016
- Microsoft Office Web Apps 2010, 2013
- Microsoft Office Online Server

RISK:

Government:

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

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY

Multiple vulnerabilities have been discovered in Microsoft Office, the most severe of which could allow for remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited these vulnerabilities could run arbitrary code in the context of the current user.

- Six memory corruption vulnerabilities exist when the Office software fails to properly handle objects in memory. (CVE-2016-3278, CVE-2016-3280, CVE-2016-3281, CVE-2016-3282, CVE-2016-3283, CVE-2016-3284)
- A remote code execution vulnerability exists when Office fails to properly handle XLA files. (CVE-2016-3279)

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. 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.

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.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/MS16-088>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3278>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3279>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3280>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3281>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3282>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3283>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3284>

TLP: WHITE

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

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