

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:

03/08/2015

SUBJECT:

Multiple Vulnerabilities in Microsoft Office Could Allow for Remote Code Execution (MS16-29)

EXECUTIVE 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. 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 Office 2007, 2010, 2013, 2013 RT, 2016
- Microsoft Office Mac 2011 and 2016 for Mac
- Microsoft SharePoint Server 2010, 2013
- Microsoft Office Web Apps 2010, 2013

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 exist in Microsoft Office, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Two remote code execution vulnerabilities exist in Microsoft Office software when the Office software fails to properly handle objects in memory. An attacker who successfully exploited these vulnerabilities could run arbitrary code in the context of the current user. Note that the Preview Pane is not an attack vector for these vulnerabilities. Successful exploitation of these

vulnerabilities could result in an attacker gaining the same privileges as the logged on user. (CVE-2016-0021, CVE-2016-0134)

- A security feature bypass vulnerability exists in Microsoft Office software due to an invalidly signed binary. An attacker who successfully exploited the vulnerability could use a similarly configured binary to host malicious code. A defender would then not be able to rely on a valid binary signature to differentiate between a known good and a malicious binary. To successfully exploit this vulnerability, an attacker would have to have write access to the target location that contains the invalidly signed binary. The attacker could then overwrite the original file with their own malicious file and wait for an application, or user, to trigger the malicious binary. (CVE-2016-0057)

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. Customers 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.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/MS16-029>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0021>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0057>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0134>

TLP: WHITE

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

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