

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/>

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Keynote, Pages, and Numbers that could lead to remote code execution. Keynote is used to prepare presentations on Apple platforms. Pages is a word processing software for the Apple platform and the Numbers application is used to work with spreadsheets.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and the ability to bypass the security system. 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 currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- OS X Yosemite v10.10.4 or later
- iOS 8.4 or later

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: High

TECHNICAL SUMMARY:

Multiple Vulnerabilities have been discovered in Keynote, Pages, and Numbers. The most serious of these vulnerabilities could lead to remote code execution. Details of these vulnerabilities are as follows:

- Multiple input validation issues existed in parsing a maliciously crafted document. These issues were addressed through improved input validation. (CVE-2015-3784, CVE-2015-7032)
- Memory corruption vulnerability for Keynote, Pages, and Numbers could allow for arbitrary code execution when opening a maliciously crafted document. (CVE-2015-7033)

- Memory corruption vulnerability for Pages could allow for arbitrary code execution when opening a maliciously crafted document. (CVE-2015-7034)

Successful exploitation could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and the ability to bypass the security system. 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.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Apple 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 download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Apple:

<https://support.apple.com/en-us/HT205373>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3784>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7032>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7033>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7034>

TLP: WHITE

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

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