

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:

04/27/2015

SUBJECT:

Vulnerability in Apache OpenOffice and LibreOffice Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in LibreOffice and Apache OpenOffice which could allow for remote code execution. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged-on user and allow for the execution of arbitrary code.

THREAT INTELLIGENCE

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Apache OpenOffice 4.1.1 and prior
- LibreOffice versions other than 4.3.7 and 4.4.2

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:

A vulnerability in OpenOffice and LibreOffice Hangul Word Processor (HWP) filters has been confirmed by each vendor. This vulnerability could be exploited

by opening a specially crafted HWP formatted document (".hwp") via an e-mail attachment. When a user running a vulnerable version of the product opens a HWP document, malicious code could then be executed.

Successful exploitation 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.

RECOMMENDATIONS:

The following actions should be taken:

- LibreOffice users should update to the latest version of LibreOffice after appropriate testing.
- OpenOffice is anticipating a fix in version 4.1.2, not yet released, but offers a workaround solution. Refer to the Apache OpenOffice advisory referenced below.
- Run all software as a non-privileged user to diminish effects of a successful attack.
- Remind users not to click links or open attachments from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Apache OpenOffice:

<http://www.openoffice.org/security/cves/CVE-2015-1774.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2015-1774>

LibreOffice:

<https://www.libreoffice.org/about-us/security/advisories/cve-2015-1774/>

Security Focus:

<http://www.securityfocus.com/bid/74338>

TLP: WHITE

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

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