

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:

03/02/2015

SUBJECT:

Vulnerability in Microsoft Word Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

A memory corruption vulnerability has been discovered in Microsoft Word that could allow for remote code execution. An attacker can exploit this issue to execute arbitrary code in the context of the currently logged-in user. Failed exploit attempts will likely result in denial-of-service conditions.

THREAT INTELLIGENCE:

At this time, CIS has not observed this attack being used in the wild.

SYSTEM AFFECTED:

- Microsoft Word

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 memory corruption vulnerability has been discovered in Microsoft Word that could allow for remote code execution. Specifically, this issue exists in the line formatting functionality of Microsoft Word. To exploit this issue, an attacker would need to entice an unsuspecting user to view a specially crafted Word file. Successful exploitation of this vulnerability could allow attackers to execute arbitrary code in the context of the currently logged-in user. Failed exploit attempts will likely result in denial-of-service conditions.

Please note that there is currently no patch available for this vulnerability. We will update this advisory with additional information as soon as we receive it.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the patch from Microsoft, as soon as one becomes available, 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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

ZeroDayInitiative:

<http://www.zerodayinitiative.com/advisories/ZDI-15-052/>

SecurityFocus:

<http://www.securityfocus.com/bid/72823>

TLP: WHITE

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

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