

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.

DATE(S) ISSUED:

06/10/2014

SUBJECT:

Memory Corruption Vulnerability in Microsoft Word Could Allow Remote Code Execution (MS14-034)

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.

SYSTEM AFFECTED:

- Microsoft Office 2007 SP3
- Microsoft Office Compatibility Pack SP3

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 occurs when Microsoft Word parses a specially crafted Office file.

To exploit this issue, an attacker would need to entice an unsuspecting user to view the specially crafted Office 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.

RECOMMENDATIONS:

The following actions should be taken:

- 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:

Microsoft:

<https://technet.microsoft.com/library/security/ms14-034>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1761>