

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:

02/12/2013

SUBJECT:

Vulnerability in OLE Automation Could Allow Remote Code Execution (MS13-0020)

OVERVIEW:

A vulnerability has been discovered in Microsoft Windows Object Linking and Embedding (OLE) Automation which could allow an attacker to take complete control of an affected system. Microsoft Object Linking and Embedding (OLE) Automation is an inter-process communication mechanism used by languages that run on Windows. It provides an infrastructure for automation controllers to access and manipulate (i.e. set properties of or call methods on) shared automation objects that are exported by other applications.

The vulnerability could allow remote code execution if a user opens a specially crafted file. Successful exploitation of this vulnerability could allow the attacker to could gain the same user rights as the current user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft Windows XP Service Pack 3

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

DESCRIPTION:

A vulnerability has been discovered in Microsoft Windows Object Linking and Embedding (OLE) Automation. This remote code execution vulnerability exists in the way that Object Linking and Embedding (OLE) Automation parses specially crafted data. The vulnerability could allow

remote code execution if a user opens a specially crafted file. Successful exploitation of this vulnerability could allow the attacker to could gain the same user rights as the current 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 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.
- Remind users not to visit un-trusted websites, follow links, or open files provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-020>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1313>