

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:

09/10/2013

SUBJECT:

Vulnerabilities in Microsoft Access Could Allow Remote Code Execution (MS13-074)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's database software, Access, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities 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.

SYSTEM AFFECTED:

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013

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:

Three vulnerabilities have been privately reported in Microsoft Access. These vulnerabilities can be triggered by opening a specially crafted Access file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted Access file as an email attachment. In the web based scenario, a user would have to open the specially crafted Access file that is hosted on a website. When the user opens the Access file, the attacker's supplied code will execute. Details of these vulnerabilities are as follows:

File Format Memory Corruption Vulnerability

One remote code execution vulnerabilities exist in the way Access handles memory when opening specially crafted Access files.

Memory Corruption Vulnerabilities

Two remote code execution vulnerabilities exist in the way Access accesses objects in memory that have not been properly initialized or deleted.

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:

- 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 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/en-us/security/bulletin/ms13-074>

Security Focus:

<http://www.securityfocus.com/bid/62229>

<http://www.securityfocus.com/bid/62230>

<http://www.securityfocus.com/bid/62231>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-32155>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-32156>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-32157>