

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:

8/13/2013

SUBJECT:

Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (MS13-061)

OVERVIEW:

Three vulnerabilities have been discovered in Microsoft Exchange Server that could allow for remote code execution or cause Denial of Service (DoS) conditions. Microsoft Exchange Server provides email, calendar and contacts for corporate environments. Successful exploitation of two of the vulnerabilities could allow an attacker to run arbitrary code on the affected Microsoft Exchange Server. Exploitation of the other vulnerability could result in a Denial of Service (DoS) condition.

SYSTEMS AFFECTED:

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 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: N/A

DESCRIPTION:

Three vulnerabilities have been discovered in Microsoft Exchange Server. Two of the vulnerabilities, CVE-2013-2393 and CVE-2013-3776, occur because of the way the WebReady Document Viewing service parses files using the Oracle Outside In libraries. This issue exists due to vulnerabilities contained within the libraries themselves. MS Exchange Server WebReady Document viewing is a feature that allows Outlook Web Access (OWA) users to view attachments such as Microsoft Office documents within the browser. WebReady Document viewing is enabled by default. These vulnerabilities can allow an attacker to run code on the Windows Exchange Server under the context of the LocalService account. If

disabled, OWA users may not be able to preview the content of email attachments. To exploit this vulnerability, an attacker must create a specially crafted file that is sent via e-mail to a user on a vulnerable version of Microsoft Exchange Server. When the user previews the document by clicking on the "Open as Webpage" link within OWA, the attacker's code runs within the privilege context of the LocalService account on the Microsoft Exchange Server. The LocalService account by default has limited system and file system privileges and sends only anonymous credentials over the network.

The third vulnerability, CVE-2013-3781, exists only in Exchange Server 2013 through the Data Loss Prevention (DLP) feature. This vulnerability could cause the affected Exchange server to become unresponsive if a user views a specially crafted file through Outlook Web Access, resulting in Denial of Service conditions.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Evaluate the need for WebReady Document viewing and disable if deemed non-essential.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open un-trusted attachments from unknown or untrusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/security/bulletin/ms13-061>

<https://support.microsoft.com/kb/2876063>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2393>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3776>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3781>