

*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:**

Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (MS13-012)

**OVERVIEW:**

Two vulnerabilities have been reported in Microsoft Exchange Server that could allow for remote code execution or Denial of Service (DoS) conditions. Microsoft Exchange Server provides email, calendar and contacts for corporate environments. Successful exploitation of one of the vulnerabilities could allow an attacker to run arbitrary code within the context of the LocalService account on the affected Microsoft Exchange Server. Typically, the LocalService account has minimum privileges on the system. Exploitation of the other vulnerability could cause Denial of Service (DoS) conditions.

**SYSTEMS AFFECTED:**

Microsoft Exchange Server 2007  
Microsoft Exchange Server 2010

**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:**

Two vulnerabilities have been discovered in Microsoft Exchange Server. These vulnerabilities occur in the way the WebReady Document Viewing service parses files using the Oracle Outside In libraries. These issues exist due to vulnerabilities contained within libraries of Oracle Outside In.

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. The vulnerability outlined in CVE-2013-

0418 can allow an attacker to run code on the Windows Exchange Server under the context of the LocalService account. The vulnerability described in CVE-2013-0393 can allow an attacker to create a denial of service condition on the Windows Exchange Server. If disabled, OWA users may not be able to preview the content of email attachments.

To exploit these vulnerabilities, an attacker creates 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, an attacker's code may run 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. Attacks exploiting CVE-2013-0393 may cause the Microsoft Exchange Server they become unresponsive creating a denial of service condition.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems after testing.
- Evaluate the relative 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/ms13-012>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0418>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0393>