

*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:**

02/11/2014

**SUBJECT:**

Vulnerability in Microsoft Forefront Protection for Exchange Could Allow Remote Code Execution (MS14-008)

**EXECUTIVE SUMMARY:**

A vulnerability has been found in Microsoft Forefront Protection for Exchange 2010 that could allow an attacker to take complete control of an affected system. Microsoft Forefront Protection provides defense against malware and spam by scanning emails and attachments for malicious content. 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.

**THREAT INTELLIGENCE:**

At this time these vulnerabilities are not publicly disclosed and there is no known proof-of-concept code available.

**SYSTEM AFFECTED:**

- Microsoft Forefront Protection 2010 for Exchange Server

**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 vulnerability has been privately reported to Microsoft that could allow for remote code execution within the Microsoft Forefront Exchange Server add-on. This vulnerability results in remote code execution when a mail parsing error occurs from Microsoft Forefront scanning a specially crafted email.

Successful exploitation could result in an attacker gaining the same privileges as the service account Microsoft Exchange was being run. 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/ms14-008>

##### **CVE:**