

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:

10/08/2013

SUBJECT:

Vulnerabilities in .NET Framework Could Allow Remote Code Execution (MS13-082)

OVERVIEW:

Multiple vulnerabilities have been discovered in the Microsoft .NET Framework which could allow an attacker to take complete control of an affected system. Microsoft .NET is a software framework for applications designed to run under Microsoft Windows.

These vulnerabilities can be exploited if a user visits or is redirected to a malicious web page that contains a specially crafted OpenType font (OTF) file, while using a browser that supports XBAP applications. 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.

SYSTEMS AFFECTED:

- Windows XP
- Windows Vista
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows 7
- Windows 8
- Windows RT
- Microsoft .NET Framework 4.5 and earlier for Windows

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:

Multiple vulnerabilities have been discovered in the Microsoft .NET Framework which could allow an attacker to take complete control of an affected system. These vulnerabilities are as follows:

OpenType Font Parsing Vulnerability (CVE-2013-3128)

A remote code execution vulnerability exists in the way that affected components handle specially crafted OpenType fonts (OTF). The vulnerability could allow remote code execution if a user visits a website hosting an XAML Browser Application (XBAP) containing a specially crafted OTF file.

Entity Expansion Vulnerability (CVE-2013-3860)

A denial of service vulnerability exists in the .NET Framework that could allow an attacker to cause a server or application to crash or become unresponsive.

JSON Parsing Vulnerability (CVE-2013-3861)

A denial of service vulnerability exists in the .NET Framework that could allow an attacker to cause a server or application to crash or become unresponsive.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all services.
- Unless there is a business need to do otherwise, consider disabling Microsoft .NET applications.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/security/bulletin/ms13-082>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3128>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3860>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3861>