

*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.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

08/11/2015

**SUBJECT:**

Multiple vulnerabilities in Microsoft Remote Desktop Protocol Could Allow for Remote Code Execution (MS15-082)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Remote Desktop Protocol (RDP), the most severe of which could allow attackers to take complete control of affected systems. The Remote Desktop Protocol provides a graphical interface for users to establish a virtual session to other computers. Successfully exploiting these vulnerabilities could then allow the attacker to install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in Denial of Service conditions on targeted systems.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

It should be noted that the MS-ISAC has historically identified a large amount of scanning for RDP service as well as brute force attempts against systems running this service.

**SYSTEM AFFECTED:**

- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008 (Server Core Installations Are Affected)
- Windows Server 2012 (Server Core Installations Are Affected)
- Windows RT

**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: Low**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Remote Desktop Protocol (RDP), the most severe of which could allow attackers to take complete control of affected systems. By default, RDP is not enabled on any Windows operating systems. These vulnerabilities are either caused by the way RDP validates certificates during authentication or processes a specially crafted RDP file.

A remote unauthenticated attacker could only exploit these vulnerabilities if the RDP server service is enabled. The exploitation of these issues could lead to the execution of arbitrary code on the target

system which could then allow the attacker to install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in Denial of Service conditions on targeted systems.

**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.
- Block TCP/UDP port 3389 at the perimeter firewall if there is no documented business need.

**REFERENCES:**

**Microsoft:**

<https://technet.microsoft.com/library/security/ms15-082>

**CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2472>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2473>

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>