

*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:**

06/12/2012

**SUBJECT:**

Vulnerability in Remote Desktop Protocol Could Allow Remote Code Execution (MS12-036)

**OVERVIEW:**

A vulnerability in Remote Desktop Protocol (RDP) could allow attackers to take complete control of affected systems or cause a Denial-of-Service. The Remote Desktop Protocol provides a graphical interface for users to establish a virtual session to other computers. Successfully exploiting this vulnerability would 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.

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.

**SYSTEMS AFFECTED:**

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

**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**

**DESCRIPTION:**

A vulnerability has been identified in the Remote Desktop Protocol (RDP) that could allow attackers to either take complete control of affected systems or cause a Denial-of-Service. By default, RDP is not enabled on any Windows Operating systems. This vulnerability is caused by the way the Remote Desktop Protocol processes a sequence of specially crafted packets, resulting in the access of an object in memory that has not been properly initialized or has been deleted. A remote unauthenticated attacker could exploit this vulnerability only if RDP is enabled. The exploitation of this issues could lead to an attacker running arbitrary code on the target system. Successfully exploiting this vulnerability would then allow the attacker to install programs; view, change, or delete data; or create new accounts with full user rights.

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.

**RECOMMENDATIONS:**

The following actions should be taken:

Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

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

Disable Terminal Services, Remote Desktop, Remote Assistance, and Windows Small Business Server 2003 Remote Web Workplace feature if no longer required.

**REFERENCES:**

**Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-036>

**Security Focus:**

<http://www.securityfocus.com/bid/53826>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0173>