

*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:**

3/13/2012

**SUBJECT:**

Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (MS12-020)

**OVERVIEW:**

Multiple vulnerabilities in Windows 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 hosts on the network. 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. This could also result in producing a Denial of Service condition on targeted systems.

Please note that Microsoft is strongly encouraging entities to make a special priority of applying this particular update. The MS-ISAC, via the MSS and Albert services, 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:**

New vulnerabilities have been reported 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.

One vulnerability is caused by to 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. An attacker could exploit this vulnerability only if RDP is enabled and:

- If the operating system is Windows XP or Windows Server 2003, a remote unauthenticated attacker could exploit this vulnerability.
- If the operating system is Windows Vista, Windows 7, or Windows Server 2008 and Network Level Authentication is turned off, a remote unauthenticated attacker could exploit this vulnerability.

- If the operating system is Windows Vista, Windows 7, or Windows Server 2008 and Network Level Authentication is turned on in RDP, an attacker would have to authenticate with a valid account in order to exploit this vulnerability.

The exploitation of these 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.

The second vulnerability is caused due to the way Remote Desktop Protocol processes a sequence of specially crafted packets, resulting in a Denial of Service condition.

Please note that Microsoft is strongly encouraging entities to make a special priority of applying this particular update. The MS-ISAC, via the MSS and Albert services, 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.
- Disable Terminal Services, Remote Desktop, Remote Assistance, and Windows Small Business Server 2003 Remote Web Workplace feature if no longer required.
- Enable Network Level Authentication on systems running supported editions of Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2.

### **REFERENCES:**

#### **Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-020>

<http://support.microsoft.com/kb/2671387>

#### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152>

#### **Security Focus:**

<http://www.securityfocus.com/bid/52353>

<http://www.securityfocus.com/bid/52354>