

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:

07/14/2015

SUBJECT:

Vulnerability in Microsoft Remote Desktop Protocol Could Allow for Remote Code Execution (MS15-067)

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 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 7
- Windows 8
- Windows Server 2012

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:

A vulnerability has been identified in the RDP that could allow attackers to either take complete control of affected systems or cause a Denial of Service event. By default, RDP is not enabled on any Windows Operating systems. This vulnerability is caused by the way RDP processes a sequence of specially crafted packets.

A remote unauthenticated attacker could only exploit this vulnerability if the RDP server service is enabled. The exploitation of this issue 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.

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

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms15-067.aspx>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2327>

TLP: WHITE

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

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