**Alert – Remote Desktop services Remote Code Execution vulnerability**

**Description/Overview:**

A Vulnerability has been discovered in Remote Desktop Services and is identified as ***"CVE-2019-0708 – Remote Desktop Services Remote Code Execution Vulnerability*** – formerly known as Terminal Services.

**Impact**:

1. This vulnerability is 'wormable', meaning that **any future malware that exploits this vulnerability could propagate from one vulnerable computer to another vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017.** While there is no observed exploitation of this vulnerability yet, it is highly likely that malicious actors will write an exploit for this vulnerability and incorporate it into their malware.
2. When an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

**Vulnerable or affected versions:**

– Microsoft Windows 7 SP1

– Windows Server 2008 SP2

– Windows Server 2008 R2 – SP1

– Windows XP (All Versions)

– Windows Server 2003 SP2

**Solution:**

Rw-CSIRT is strongly recommending **users** and **IT administrators** to follow the

instructions below:

**To patch their systems immediately, if they have any of the following affected Windows versions in use:**

– Microsoft Windows 7 SP1

– Windows Server 2008 SP2

– Windows Server 2008 R2 – SP1

– Windows XP (All Versions)

– Windows Server 2003 SP2

If one cannot apply the Security Updates provided by Microsoft immediately, they should consider disabling the Remote Desktop Services on the vulnerable hosts until official patches are applied.

**Affected users should**: contact RW-CSIRT: Call **4045** or write to **security@risa.gov.rw** to help for analyzing the source of the incident and recommendation.

**Vulnerability Details:**
https://blogs.quickheal.com/cve-2019-0708-critical-wormable-remote-code-execution-vulnerability-windows-rdp/

**References:**

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708#ID0EMGAC
- https://blogs.quickheal.com/cve-2019-0708-critical-wormable-remote-code-execution-vulnerability-windows-rdp/
- https://twitter.com/e_kaspersky/status/1130538594584748032?s=08

**National Computer Security and Incident Response Team (Rw-CSIRT) Mission**

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of "early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability" and raise cyber security awareness in public.