Global Product Security Announcement

REMOTE DESKTOP PROTOCOL (RDP) AND THE INTERNET WHAT ARE THE RISKS OF EXPOSURE

The Remote Desktop Protocol, commonly referred to as RDP, is a proprietary protocol developed by the Microsoft Corporation that provides a graphical means of connecting to a network-connected computer. RDP client and server support has been present in varying capacities in most every Windows® Operating System (OS) version since the Windows NT® OS. The default RDP configuration on older versions of the Windows OS left it vulnerable to several attacks when enabled; newer versions have improved its security but it's still not enough on its own.

It's convenient to use the RDP for accessing systems over the Internet especially in server environments; however, exposing RDP to direct connections is risky. This setup not only gives remote attackers the opportunity to guess logon credentials, but its security posture also relies on the lack of a remotely exploitable vulnerability in the Microsoft® RDP implementation. Unfortunately, the Microsoft RDP implementation already has a remotely exploitable vulnerability. The Microsoft Security Bulletin MS12-020, released in March 2012, described critical vulnerability in Microsoft's RDP implementation on most Windows platforms (CVE-2012-0002). This vulnerability allows a remote unauthenticated attacker to run arbitrary code on the affected system by sending a sequence of specially crafted RDP packets.

Let's make one thing clear: there are situations in which using some sort of remote administration utility is an absolute necessity. But in any other case, you should avoid this kind of software if you are concerned about the security of your system. If you must connect remotely to another computer's desktop environment, do it through a Virtual Private Network (VPN). Otherwise, you're practically communicating out in the open and "anything goes." Using an open connection allows malware to "call home" and gives hackers an opening to try to infiltrate your system.

Since 2002, there have been at least 20 Microsoft security updates specifically related to RDP and at least 24 separate vulnerability announcements. Some of them are listed here:

MS01-052	MS05-041	MS11-017	MS11-065	MS12-036	MS13-029
MS02-051	MS09-044	MS11-061	MS12-020	MS12-053	MS14-030
MS14-074	MS15-030	MS15-067	MS15-082	MS16-017	MS16-067

Due to the number of vulnerabilities and sophistication of attackers, we strongly encourage our customers and service professionals to always protect customers' systems and not to expose their systems directly to the Internet. We recommend the use of VPN or other technologies to manage accounts and further protect our customers from malicious attackers.

If you have any questions, you can contact us at productsecurity@jci.com