SearchSecurity.com

Attack code surfaces for Microsoft RDP vulnerabilities

Proof-of-concept code has surfaced on several Chinese websites targeting the recently patched Windows Remote Desktop Protocol (RDP) vulnerabilities, according to security researchers and antimalware vendors that track new exploit code.

> RDP has a lot of implications. The fact that many people are running that and it's available through the Internet-- that's actually kind of a scary one to me.
>
> Marcus Carey,
> security researcher at Rapid7

McAfee, SophosLabs, Symantec and Kaspersky Lab have issued warnings to IT administrators in charge of their companies' patching activities: Update your systems or face the possibility of a network worm attack.

"Patch your copies of Windows as soon as possible," wrote Graham Cluley of Sophos' Naked Security blog. "Windows users should consider themselves on high alert and harden their defenses."

The RDP vulnerability, which affects all Windows systems, is the only "critical" update issued by Microsoft in its March 2012 Patch Tuesday release. Microsoft RDP provides remote display and input capabilities over the network for Windows-based applications. It is not enabled by default but many organizations have it enabled because it's a key component used by remote desktop software. For example, a presentation can be viewed in real-time to multiple Windows users without having to send the same data to each session individually. The RDP flaws can be used by attackers to install malware and crash a Windows system or server. The update affects all Microsoft Windows operating systems and servers.

Code leak from Microsoft?
Security researchers suspect that the proof-of-concept code that surfaced may be connected to Microsoft's Active Protection Program (MAPP). The program is used by trusted security vendors to add protections against attacks targeting new Microsoft vulnerabilities into intrusion defense and other security systems.

Luigi Auriemma, who discovered the Microsoft RDP vulnerability noted that the proof-of-concept exploits he examined appeared to use the same coding he sent to the TippingPoint Zero Day Initiative. There is still no word from Microsoft corroborating the finding.

Microsoft engineers Suha Can and Jonathan Ness, writing on the Microsoft Security Research and Defense blog, warned that an exploit would be created quickly.

"Developing a working exploit will not be trivial: we would be surprised to see one developed in the next few days," the MSRC engineers said. "However, we expect to see working exploit code developed within the next 30 days."

The proof-of-concept code appears to make a Windows system crash. Some security experts say it's the first step before an attacker creates a network worm.

For users of Windows Vista, Server 2008, Win7 and Server 2008 R2 systems, Microsoft has issued a one-click, no-reboot fix that will mitigate the issue. The update would enable Network-Level Authentication, preventing an attacker from targeting the vulnerabilities without credentials.

"We strongly recommend that customers examine and prepare to apply this bulletin as soon as possible," wrote Angela Gunn, a spokesperson with Microsoft Trustworthy Computing.