Threat Assessment: Terminal Services RDP Vulnerability

David Holmes, 2012-19-03

#adcfw #infosec

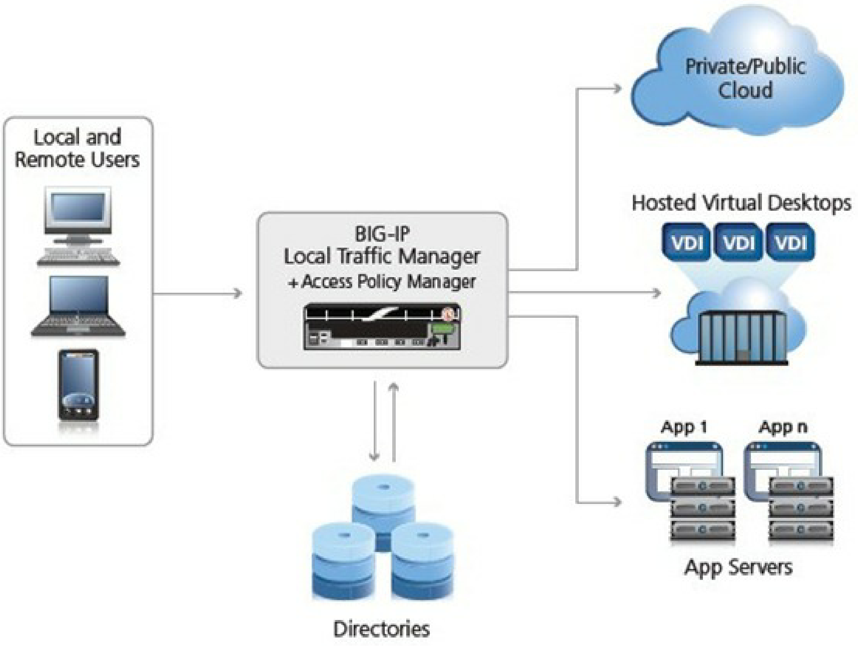
Remember the bad old days before Remote Desktop Protocol (RDP), when the Virtual Network Computing (VNC) viewer didn't even offer confidentiality (fancy word for encryption)? VNC was a still useful tool, so everyone would learn how to use SSH tunnels just long enough to configure the tunnel before forgetting the syntax again. Eventually the RDP protocol took over and offered the right mix of performance, ease-of-use, and confidentiality. And in the Windows world, RDP has been the de-facto remote access standard for quite some time.

Beginning with Terminal Services server in Windows NT 4.0, RDP has been included with every version of Microsoft's server operating system including the latest, Windows Server 2008 R2. In addition to providing RDP clients, with names such as terminal services client and remote desktop connection, in every Microsoft client operating system since Windows XP to connect to RDP servers, use of the protocol has also manifested itself as Remote Assistance (RA). RA functions a bit differently however, requiring a user to be present and to accept the incoming connection.

The widespread use of RDP makes the announcement last week of **Security Bulletin MS12-020** particularly significant. The critically rated MS12-020 is a "use-after-free" memory corruption issue that could lead to remote code execution. This type of vulnerability occurs when an object's memory is freed without cleaning up remaining references to it. If a reference is used later, the "invalid memory" is instantiated as a valid object, and in the case of exploitation, could lead to the execution of arbitrary code. Note that Internet Explorer was susceptible to the same class of bug last year (see MS11-018).

There are at least two proof-of-concept exploit demos in the wild; we've seen one in written in Ruby and another one in Python. There's also been at least one hoax exploit that was posted to Pastebin the middle of last week.

Microsoft's suggested mitigation until the issue can be patched is to disable RDP/TS or block port 3389 at the network perimeter. Of course, one security solution, which many of you are probably employing already, is to use a VPN of some kind to pre-authenticate and encrypt your RDP sessions.



F5 mitigation via BIG-IP Access Policy Manager

The F5 Threat Analysis Team has done an assessment of how our products interact with this vulnerability. The **Access Policy Manager** (APM) provides protection against MS12-020. With APM configured as an RDP proxy, a user has to authenticate (successfully) before they are connected to the back-end RDP service. This prevents unauthorized users from exploiting another user's session. This isn't to say that an authenticated user couldn't perform this attack for privilege escalation purposes, but if they did you'd at least know who they were via the audit trail and you could take whatever steps are appropriate.

Over the weekend, Dan Kaminisky scanned 8% of the Internet and is approximating that there are roughly 5 million machines listening to port 3389/tcp right now. He makes a good point about how it is not necessarily constructive to shame the victim at a time like this.

> "If you have any sort of crisis response policy, and you aren't completely sure you're safe from the RDP vulnerability, I advise you to invoke it as soon as possible." – Dan Kaminsky

Given the sheer number of exposed machines and the potential severity of this vulnerability, that's probably a good idea.

v11: RDP Access via BIG-IP APM

Getting at the Heart of Security in the Cloud

Identify the Most Probable Threats to an Organization

BIG-IP Access Policy Manager (APM) Wiki