Summary: On Tuesday March 13th Microsoft released MS12-020 concerning vulnerabilities in RDP. This vulnerability is now being actively exploited with at least four variations as of this email. One is a DoS exploit which is trivial in complexity, but very effective at taking a system down. The remaining three allow an unauthenticated attacker to execute arbitrary code on the targeted system. Current metrics from the IPS show we normally see between 150 and 250 malicious RDP attempts in a 24 hour period. This has escalated to 689 attempts in the last 24 hours. See the end of this document for information on all Microsoft bulletins in this month’s release.

Recommendations: Expedite patch review and push to our systems.

*Note: Microsoft’s suggested fixit workaround with NLA has resulted in some systems not being able to receive connections from RDP.

Additional Links:
Microsoft: [http://support.microsoft.com/kb/2621440](http://support.microsoft.com/kb/2621440)
SANs: [http://isc.sans.edu/diary.html?storyid=12805#comment](http://isc.sans.edu/diary.html?storyid=12805#comment)

Current list of affected systems: (seems to be increasing with updates from various vendors)

- Avaya Aura Conferencing 6.0 SP1 Standard
- Avaya Aura Conferencing 6.0 Standard
- Avaya CallPilot 4.0
- Avaya CallPilot 5.0
- Avaya Communication Server 1000 Telephony Manager 3.0
- Avaya Communication Server 1000 Telephony Manager 4.0
- Avaya Meeting Exchange - Client Registration Server
- Avaya Meeting Exchange - Recording Server
- Avaya Meeting Exchange - Streaming Server
- Avaya Meeting Exchange - Web Conferencing Server
- Avaya Meeting Exchange - Webportal
- Avaya Meeting Exchange 5.0
- Avaya Meeting Exchange 5.0 SP1
- Avaya Meeting Exchange 5.0 SP2
- Avaya Meeting Exchange 5.0.0.0.52
- Avaya Meeting Exchange 5.1
- Avaya Meeting Exchange 5.1 SP1
- Avaya Meeting Exchange 5.2
- Avaya Meeting Exchange 5.2 SP1
- Avaya Meeting Exchange 5.2 SP2
- Avaya Messaging Application Server 4
- Avaya Messaging Application Server 5
- Avaya Messaging Application Server 5.2
- Microsoft Windows 7
- Microsoft Windows 7 Home Premium
- Microsoft Windows 7 Home Premium - Sp1 X32
- Microsoft Windows 7 Home Premium - Sp1 X64
- Microsoft Windows 7 Professional
- Microsoft Windows 7 Starter
- Microsoft Windows 7 Ultimate
- Microsoft Windows 7 for 32-bit Systems
- Microsoft Windows 7 for 32-bit Systems SP1
- Microsoft Windows 7 for x64-based Systems
- Microsoft Windows 7 for x64-based Systems SP1
- Microsoft Windows Server 2003 Datacenter Edition
- Microsoft Windows Server 2003 Datacenter Edition Itanium
- Microsoft Windows Server 2003 Datacenter Edition Itanium SP1
- Microsoft Windows Server 2003 Datacenter Edition Itanium SP1 Beta 1
- Microsoft Windows Server 2003 Datacenter Edition SP1
- Microsoft Windows Server 2003 Datacenter x64 Edition
- Microsoft Windows Server 2003 Datacenter x64 Edition SP2
- Microsoft Windows Server 2003 Enterprise Edition
- Microsoft Windows Server 2003 Enterprise Edition Itanium
- Microsoft Windows Server 2003 Enterprise Edition Itanium SP1
- Microsoft Windows Server 2003 Enterprise Edition Itanium SP1 Beta 1
- Microsoft Windows Server 2003 Enterprise Edition Itanium SP2
- Microsoft Windows Server 2003 Enterprise Edition SP1
- Microsoft Windows Server 2003 Enterprise Edition SP1 Beta 1
- Microsoft Windows Server 2003 Enterprise x64 Edition
- Microsoft Windows Server 2003 Enterprise x64 Edition SP2
- Microsoft Windows Server 2003 Itanium
- Microsoft Windows Server 2003 Itanium SP1
- Microsoft Windows Server 2003 Itanium SP2
- Microsoft Windows Server 2003 SP1
- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2003 Standard Edition SP1
- Microsoft Windows Server 2003 Standard x64 Edition
- Microsoft Windows Server 2003 x64 SP1
- Microsoft Windows Server 2003 x64 SP2
- Microsoft Windows Server 2008 Datacenter Edition
- Microsoft Windows Server 2008 Datacenter Edition SP2
- Microsoft Windows Server 2008 Enterprise Edition
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 R2 Datacenter
- Microsoft Windows Server 2008 R2 Datacenter SP1
- Microsoft Windows Server 2008 R2 Enterprise Edition
- Microsoft Windows Server 2008 R2 Itanium
- Microsoft Windows Server 2008 R2 Itanium SP1
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2008 R2 Standard Edition
- Microsoft Windows Server 2008 R2 x64
- Microsoft Windows Server 2008 R2 x64 SP1
- Microsoft Windows Server 2008 Standard Edition R2 SP1
- Microsoft Windows Server 2008 Standard Edition SP2
- Microsoft Windows Server 2008 Standard Edition X64
- Microsoft Windows Server 2008 for 32-bit Systems
- Microsoft Windows Server 2008 for 32-bit Systems SP2
- Microsoft Windows Server 2008 for Itanium-based Systems
- Microsoft Windows Server 2008 for Itanium-based Systems R2
- Microsoft Windows Server 2008 for Itanium-based Systems SP2
- Microsoft Windows Server 2008 for x64-based Systems
- Microsoft Windows Server 2008 for x64-based Systems R2
- Microsoft Windows Server 2008 for x64-based Systems SP2
- Microsoft Windows Vista Business SP1
- Microsoft Windows Vista Business SP2
- Microsoft Windows Vista Enterprise
- Microsoft Windows Vista Enterprise 64-bit edition
- Microsoft Windows Vista Enterprise 64-bit edition SP1
- Microsoft Windows Vista Enterprise 64-bit edition SP2
- Microsoft Windows Vista Enterprise SP1
- Microsoft Windows Vista Enterprise SP2
- Microsoft Windows Vista Home Basic
- Microsoft Windows Vista Home Basic 64-bit edition
- Microsoft Windows Vista Home Basic 64-bit edition SP1
- Microsoft Windows Vista Home Basic 64-bit edition SP2
- Microsoft Windows Vista Home Basic 64-bit edition Sp1 X64
- Microsoft Windows Vista Home Basic 64-bit edition Sp2 X64
- Microsoft Windows Vista Home Basic SP1
- Microsoft Windows Vista Home Basic SP2
- Microsoft Windows Vista Home Premium
- Microsoft Windows Vista Home Premium 64-bit edition
- Microsoft Windows Vista Home Premium 64-bit edition SP1
- Microsoft Windows Vista Home Premium 64-bit edition SP2
- Microsoft Windows Vista Home Premium SP1
- Microsoft Windows Vista Home Premium SP2
- Microsoft Windows Vista SP1
- Microsoft Windows Vista SP2
- Microsoft Windows Vista Ultimate
- Microsoft Windows Vista Ultimate 64-bit edition
- Microsoft Windows Vista Ultimate 64-bit edition SP1
- Microsoft Windows Vista Ultimate 64-bit edition SP2
- Microsoft Windows Vista Ultimate SP1
- Microsoft Windows Vista Ultimate SP2
COT Notification sent on March 15, 2012:

**COT Security Notification – Microsoft Security Bulletins for March 2012**

Microsoft has released 6 security bulletins. Microsoft rates 1 Critical in severity, 4 Important in severity and 1 Moderate in severity.

Microsoft information may be found at the Microsoft Security TechCenter at [http://technet.microsoft.com/en-us/security/bulletin/ms12-mar](http://technet.microsoft.com/en-us/security/bulletin/ms12-mar) or for each bulletin individually in the links provided below.

**MS12-017**  
Vulnerability in DNS Server Could Allow Denial of Service (2647170)  
*Important*  

**MS12-018**  
Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653)  
*Important*  

**MS12-019**  
Vulnerability in DirectWrite Could Allow Denial of Service (2665364)  
*Moderate*  

**MS12-020**  
Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)  
*Critical*  

**MS12-021**  
Vulnerability in Visual Studio Could Allow Elevation of Privilege (2651019)  
*Important*
MS12-022   Vulnerability in Expression Design Could Allow Remote Code Execution (2651018) Important

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn’s Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/