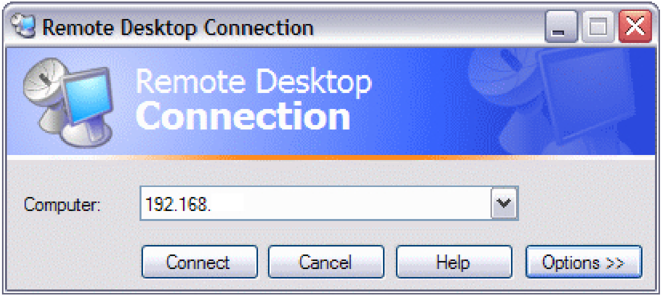
# The RDP Exploit

Matt Justice

March 21, 2012

# RDP: Remote Desktop Protocol

- Allows adminstrators to remotely control workstations & servers
- Operates on TCP port 3389.
- By default, does not require authentication to start a connection (presented with login screen).



Remote Desktop Connection

Computer: 192.168.

# The Exploit

1. Attacker crafts and sends a special RDP packet.

# The Exploit

1. Attacker crafts and sends a special RDP packet.
2. RDP mishandles the packet, resulting in DoS.

# The Exploit

1. Attacker crafts and sends a special RDP packet.
2. RDP mishandles the packet, resulting in DoS.
3. Attacker can direct the kernel to run arbitrary code.

# The Bad News

1. Exploit affects nearly every modern version of Windows, going back to XP.

# The Bad News

1. Exploit affects nearly every modern version of Windows, going back to XP.
2. Attacker does not need authentication on the network.

# The Bad News

1. Exploit affects nearly every modern version of Windows, going back to XP.
2. Attacker does not need authentication on the network.
3. The default port is rarely changed.

# The Bad News

1. Exploit affects nearly every modern version of Windows, going back to XP.
2. Attacker does not need authentication on the network.
3. The default port is rarely changed.
4. There are estimated to be $\sim$5 million RDP endpoints on the Internet.

# The Bad News

1. Exploit affects nearly every modern version of Windows, going back to XP.
2. Attacker does not need authentication on the network.
3. The default port is rarely changed.
4. There are estimated to be ∼5 million RDP endpoints on the Internet.
5. Proof of concept code already exists.

# The Bad News

1. Exploit affects nearly every modern version of Windows, going back to XP.
2. Attacker does not need authentication on the network.
3. The default port is rarely changed.
4. There are estimated to be ∼5 million RDP endpoints on the Internet.
5. Proof of concept code already exists.
6. RDP runs as the SYSTEM user, which is similar to Unix's root user.

# The Good News

1. RDP is disabled by default on workstations.

# The Good News

1. RDP is disabled by default on workstations.
2. Currently, non-Internet facing machines are safe (worm possibility!)

# The Good News

1. RDP is disabled by default on workstations.
2. Currently, non-Internet facing machines are safe (worm possibility!)
3. Exploit was patched by Microsoft on March 13 (update now!).

# Enterprise Security

1. RDP is most commonly used in enterprise environments.

# Enterprise Security

1. RDP is most commonly used in enterprise environments.
2. The RDP port is often left open through firewalls to allow administrators to remotely access machines.

# Enterprise Security

1. RDP is most commonly used in enterprise environments.
2. The RDP port is often left open through firewalls to allow administrators to remotely access machines.
3. Authentication is done after the connection creation by default.

# Sources

http://technet.microsoft.com/en-us/security/bulletin/ms12-020

http://www.symantec.com/connect/blogs/working-poc-ms12-020-spotted-wild

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0002

http://dankaminsky.com/2012/03/18/rdp/