MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Security Primer
January 2019 • SP2019-0102

Remote Desktop Protocol

Remote Desktop Protocol (RDP) is a Microsoft proprietary protocol that enables remote connections to other computers, typically over TCP port 3389. It provides network access for a remote user over an encrypted channel. Network administrators use RDP to diagnose issues, login to servers, and to perform other remote actions. Remote users use RDP to log into the organizations network to access email and files.

Cyber threat actors (CTAs) use misconfigured RDP ports that are open to the Internet to gain network access. They are then in a position to potentially move laterally throughout a network, escalate privileges, access and exfiltrate sensitive information, harvest credentials, or deploy a wide variety of malware. This popular attack vector allows CTAs to maintain a low profile since they are utilizing a legitimate network service and provides them with the same functionality as any other remote user. CTAs use tools, such as the Shodan search engine, to scan the Internet for open RDP ports and then use brute force password techniques to access vulnerable networks. Compromised RDP credentials are also widely available for sale on dark web marketplaces.

In 2018, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed an increase in ransomware variants that strategically target networks through unsecured RDP ports or by brute forcing the password. The ransomware is then manually deployed across the entire compromised network and is associated with higher ransom demands.

RECOMMENDATIONS:

- Assess the need to have RDP, port 3389, open on systems and, if required:
  - place any system with an open RDP port behind a firewall and require users to VPN in through the firewall;
  - enable strong passwords, multi-factor authentication, and account lockout policies to defend against brute-force attacks;
  - whitelist connections to specific trusted hosts;
  - restrict RDP logins to authorized non-administrator accounts, where possible. Adhere to the Principle of Least Privilege, ensuring that users have the minimum level of access required to accomplish their duties; and
  - log and review RDP login attempts for anomalous activity and retain these logs for a minimum of 90 days. Ensure that only authorized users are accessing this service.
- If RDP is not required, perform regular checks to ensure RDP ports are secured.
- Verify cloud environments adhere to best practices, as defined by the cloud service provider. After cloud environment setup is complete, ensure that RDP ports are not enabled unless required for a business purpose.
- Enable automatic Microsoft Updates to ensure that the latest versions of both the client and server software are running.

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.