Remote Desktop Access Security Finding Explainer

Security Finding Category: Remote

What did Coalition find?

Finding RDP connections on the web is like finding a screen door with a pickable lock protecting your network.

Remote Desktop Protocol can help employees access business data, but it can be an opening for hackers if improperly secured.

Security findings identified by Coalition related to Remote Desktop Protocol indicates access is exposed, accessible, and vulnerable via the public internet. This type of finding typically comes in three variations:

- Remote Desktop Protocol (RDP)
- Remote Desktop Web Access (RDWeb)
- Remote Desktop Gateway (RDGateway)

Attackers don't really care who or what is behind the door, they just see an easy target.

Why is this risky?

RDP is a network communications protocol developed by Microsoft and the underlying technology is not inherently risky if properly secured and limited internal use.

RDP, RDWeb, and RDGateway become risky when they are used as one of the primary methods for remote access and are discoverable — essentially left open — via the public internet. In this case, the same technology that makes it easier for users to access remote systems can be exploited by attackers.

Why is this an urgent issue for your client?

Coalition scans for risks that attackers are actively seeking to exploit. The pervasiveness of this issue, combined with the ease of discovery, is an ideal opportunity for those looking to commit cyber crimes.

RDP exposures continually rank among the top drivers of cyber insurance claims. **Coalition's 2023 Threat Index validates** this by identifying RDP as the top protocol attackers seek to exploit.

Because of these risks Coalition typically requires RDP and its related services to be removed from the public internet before we bind or renew a policy.

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **help@coalitioninc.com**

Now What?

As a broker, your role is not to fix this issue but to guide your client and help them prioritize remediation. RDP has known significant risks and can negatively impact insurability.

The good news is there are many resources your client can use to mitigate their RDP exposure and alternative solutions to safely replace RDP:

1. Remote Access Best Practices
2. Understanding Remote Desktop Protocol

Help your clients make cybersecurity less daunting with Control

The best way to help your client take control of their risks is to direct them to **Coalition Control™**. Coalition Control empowers your clients to strengthen their security posture by detecting, assessing, and mitigating cyber risks before they turn into events and claims.

If your client is not directly responsible for IT or security support they can grant their colleagues direct access to Coalition Control by following these simple steps:

1. From Coalition Control click on the **Invite** option in the upper right corner of the screen
2. Add the email address of your organization's Security or IT users or service providers
3. Click **Invite Now** to confirm

Still have questions?

Contingent new business quote:
Schedule a call with a Coalition Security Engineer

Existing policyholder or midterm security alert:
Email securitysupport@coalitioninc.com

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **help@coalitioninc.com**