Exposed Risky Panels (Restrict Access) Security Finding Explainer

Security Finding Category: Exposed Critical Software

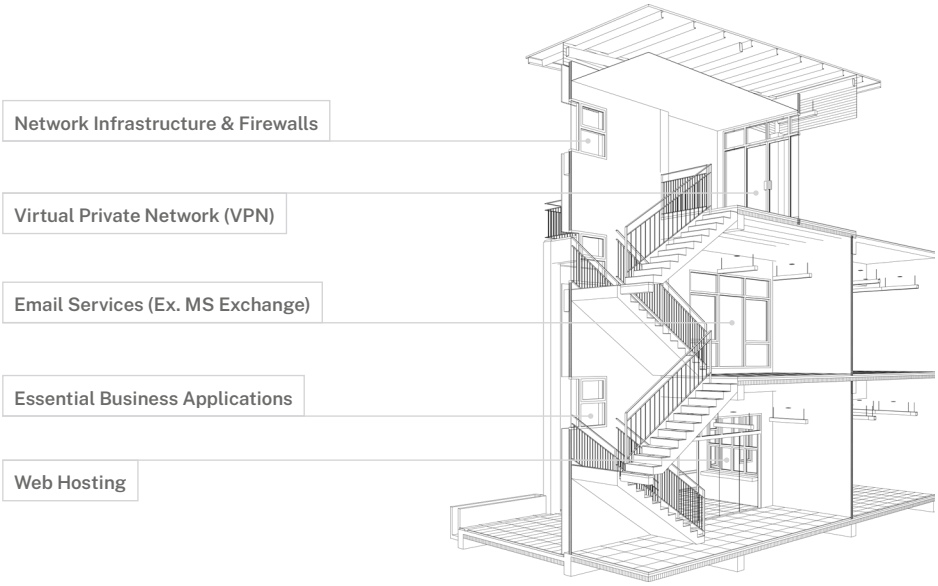
What did Coalition find?

Think of leaving admin panels exposed to the internet like leaving your door unlocked to let the repairman in when you're not home — except instead of telling them privately, you post banners on all your doors and windows that say; "Everything's open!" While the repairman will have no problem getting into your house, neither will anyone else.

If your client is alerted to "Exposed Risky Panels," it indicates Coalition's scanning found login panels accessible over the web that could expose sensitive systems or grant attackers administrative privileges. This explainer addresses the latter, also known as exposed admin panels.

Why is this risky?

Exposed admin panels give IT professionals remote access to manage the configuration, settings and features of applications and technologies for the organization. The level of access gained through the admin panels detected by Coalition poses unique risks if the access falls into the hands of malicious actors. This makes it essential that admin panels should never be exposed to the public internet, **it's just too risky.**



Examples of exposed login panels

These are just a few examples of exposed login panels that Coalition often finds during external attack surface scanning.

What's the big deal?

If Coalition can see exposed login panels over the internet, it means attackers can see them as well. That's why we alert clients before binding and during the policy term when login panels are discoverable over the web.

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

Why is this an urgent issue for your client?

The sprawl of applications adopted by businesses combined with web-accessible controls and admin panels built-in creates significant risk for all organizations. Without ongoing monitoring it can be difficult for IT teams to keep up with web-accessible admin panels, and in some cases the organization may not even know it's exposed.

Because of the significant risks Coalition typically requires organizations with exposed admin panels to remediate critical security findings before a policy is bound or renewed.

Now What?

The good news is that this risk is manageable. As a benefit to all policyholders, Coalition actively scans for admin login panels that are discoverable and potentially exploitable by attackers.

As an insurance advisor, your role is **not to fix this issue** but to guide your clients and help them prioritize reducing their attack surface by hardening their IT environment. The best way to limit this exposure is to restrict access to admin panels and take steps so that panels are not discoverable and accessible over the public internet. Best practices for remediation will vary depending on the type of application, but here are a few general mitigation strategies to consider:

- Restricting access to only your internal corporate network when possible.
- Using a Zero Trust solution that validates identity and provides the minimum level of access that authorized users need for their role.
- Using a Proxy to limit discoverability over the web.
- "IP allowlisting" to only allow access from secure public IP addresses like your home or branch office.

Brokers and policyholders don't need to do this alone. Coalition is here to provide additional guidance, support and tools to streamline the security finding resolution process.

Help your clients make cybersecurity less daunting with Control

The best way to help your clients take control of their risks is to direct them to **Coalition Control™**. Coalition Control helps empower your clients to strengthen their security posture by providing full technical details of security findings and additional support to help them mitigate 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