Exposed Risky Panels (Two Factor) Security Finding Explainer

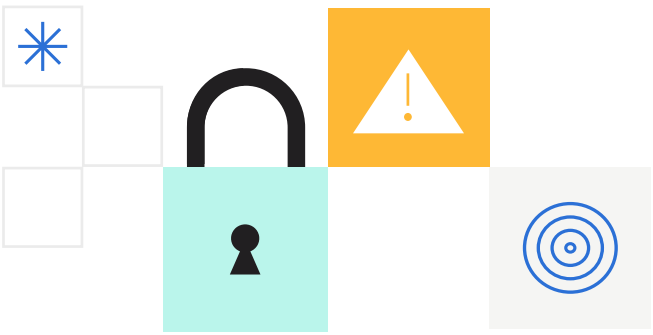
Security Finding Category: Exposed Critical Software

What did Coalition find?

Leaving login panels for essential business applications exposed to the internet and unprotected is like leaving your expensive racing bike unlocked in a busy area. You need to be able to access your bike, but you probably don't want anyone to be able to take it.

If your client receives an alert for "Exposed Risky Panels - Two Factor," it indicates Coalition's scanning found login panels for essential business applications accessible over the web but we are unable to determine if Multi-Factor Authentication (MFA) is implemented. **This finding helps confirm that this essential control is in place.**

When you use a bike for transportation, you need it to be accessible but will lock it up to prevent theft. The same applies to web-accessible login panels: locking them up keeps thieves out.



Why is this risky?

Many organizations use a mix of cloud, web, and on-premises applications in daily operations. To support the user login experience, systems are often web-accessible by default. As a result, many organizations have one or more login panels exposed to the public internet.

Web-accessible login panels pose a significant risk when they are only protected by a minimum level of security controls, usually a username and password. Attackers can use various methods to circumvent minimal security controls and gain access: using stolen or leaked credentials, brute force attacks, or a combination of phishing and keylogging designed to steal user credentials.

Why is this an urgent issue for your client?

Threat actors regularly scan the internet, looking for exposed panels to gain unauthorized access. Once inside a network, they can execute other, more devastating attacks and compromise systems and data. Without additional protections, your clients can become easy and attractive targets for attackers that could quickly turn into costly claims.

Because of this, Coalition may require confirmation that MFA is enabled on exposed risky panels before a policy is bound or renewed.

Now What?

Changes in the way we use technology and an evolving threat landscape can make it difficult for IT teams to both detect exposed login panels and keep up with security best practices.

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. Best practices for remediation will vary, but here are a few general mitigation strategies to consider:

- Ensure the latest version of the service is being used and all patches are up to date.
- Enable multi-factor authentication (MFA) controls for employees to access the panel.
- MFA and identity access management (IAM) can help secure login panels. Coalition Control has a marketplace of vendors with discounts for new signups.

If MFA is in place but not detected by our scans, this finding can be resolved by confirming that MFA is enabled and the service is patched to the latest version.

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.

If MFA is in place but not detected by our scans, this finding can be resolved by confirming that MFA is enabled and the service is patched to the latest version.

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

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