Microsoft Exchange Server Security Finding Explainer

Security Finding Category:
Exposed Critical Software

What did Coalition find?

You wouldn't leave your wallet open on the front seat of your car — the same principle is true for your digital information.

When Microsoft Exchange is discoverable by hackers over the web it can present the same risk, and you may not even know it's exposed. To make matters worse, since 2021 Microsoft has been releasing a steady stream of **critical vulnerabilities**. Some of these are even pre-authentication vulnerabilities that allow attackers to bypass basic login controls & Multi-Factor Authentication (MFA).

Security findings identified by Coalition related to Microsoft Exchange typically indicate one or more of the following panels are exposed to the public internet and vulnerable to attack:

- Microsoft Exchange and/or Exchange Admin Center (EAC)
- Exchange Web Services (EWS)
- Remote Procedure Call (RPC)

Using one of these technologies -even with basic authentication disabled -creates an enticing opportunity for hackers.

Why is this risky?

Many companies run email and calendar tools for employees using a physical Microsoft Exchange Server installed "on-premises" at one or more of their offices.

This becomes particularly risky when administrator access is made available remotely via EAC and/or when users are granted access via EWS or RPC. This makes it easy for users to access these applications remotely, but also creates an attractive vector of attack for threat actors.

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 and exploitation, makes this a high-risk exposure for your client.

Coalition claims data has consistently shown that organizations running on-premises Microsoft Exchange, which has several known critical vulnerabilities, directly correlate to an increased risk of cyber attacks and claims.

Because of these risks Coalition typically requires organizations running on-premises Microsoft Exchange to remediate critical security findings before we bind or renew a policy.

Now What?

The best long-term fix for this issue is to consider moving email and calendar functions to a secure and reliable cloud email solution. If moving to the cloud is not immediately possible organizations should follow best practices to control access to **EWS** & **RPC** panels.

There are also several technology solutions organizations can explore to minimize exposure by removing EAC, EWS and RPC from the public internet. Some examples include: Firewall Access Control Lists (ACLs), Virtual Private Network (VPN) or Proxy and Protective DNS.

Broker's 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 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**