As details on Microsoft Exchange vulnerabilities affecting thousands of organizations emerged, with aggressive attacks spiking this month, even the White House weighed in, warning that companies had "hours, not days" to fix vulnerabilities.

Much has already been said already about this critical situation — security vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) that enable attackers to gain significant access to and control over not only Exchange but also other internal systems.

And new details and reporting continue to come to light, not only from expected security sites like Krebs on Security and Microsoft itself, but also from the broader general media.

CNN and the Associated Press have all intensely spotlighted this issue; the New York Times published reports from Microsoft that as of March 16, over 80,000 internet-facing Exchange servers are still unpatched and awaiting updates.

In the midst of all of this, I wanted to share a real-world story about how Chuco worked with one client to use its existing Tanium system to quickly identify and fix Exchange issues they didn't even realize they had.

An Urgent Problem Meets Swift Response

At Chuco, we support a large national retailer generating $1.5 billion in annual revenue that has adopted several Tanium tools to help manage over 5000 endpoints.

When working with clients, we adopt an engagement model that best aligns with their priorities and preference in terms of scope of service, resource availability, and access levels. In this case, we had full access to the Tanium Console and a license to put hands on keyboard.

Because the Tanium team quickly put together a detailed guide for finding and remediating these Exchange vulnerabilities, we were able to spring into action immediately.

And it's a good thing that we did — using the detailed instructions and query language Tanium provided we were able to quickly identify a number of unpatched servers. With that list in hand, we provided the client with the exact details it needed to act quickly to plan and execute server updates.

Importantly, Tanium reported details about vulnerable Exchange servers the client wasn't aware it had in place — something that's not uncommon in complex IT environments with multiple offices, data centers, and distributed operational teams (particularly in today's Covid-driven landscape).

The Process in Greater Detail

Kudos to the Tanium team for producing an excellent walkthrough. The guidelines on their customer community portal provide step-by-step instructions for how to execute this process yourself, without having to reinvent the wheel: https://community.tanium.com/s/article/How-Tanium-Can-Help-with-the-March-2021-Exchange-Vulnerabilities-aka-CVE-2021-26855-CVE-2021-26857-CVE-2021-26858-CVE-2021-27065

Providing predefined queries and presenting clear screenshots, the Tanium article documents a very straightforward process. After conducting the search using Tanium Console with the Core Platform, supporting Tanium modules can be used to create reports for review, tracking and remediation. More importantly, Tanium Patch can be used to efficiency apply server updates.

The Lessons and the Larger Opportunity

This example offers several lessons and ideas to consider:

- When it comes to rapid visibility and action across your IT environment, there's a clear ROI with Tanium.

  While Microsoft acted rapidly to create and publish its own tools, including a stopgap "one-click" mitigation tool, Tanium provides great advantages in terms of execution, with its single platform approach to discovery, assessment and remediation.

  With Tanium Patch, organizations can rapidly implement updates and avoid navigating new tools or new processes to understand and follow, especially when time is of the essence.

- This is just the latest example of how organizations investing in Tanium can reap significant dividends, often when they're most urgently needed.

  In case of our Chuco client, we worked with the head of compliance to document the steps taken, the risk mitigated and the benefits achieved — presenting these details to their CIO as part of a broader effort to secure additional buy in for security and systems management investments.

- There's never a bad time to take a fresh look at how you can take your use of Tanium to the next level, particularly when it comes to security.

  Working with this client, we've started fresh discussions about how they can benefit from Tanium Threat Response, to better prepare for and respond to future incidents. Mapping Chuco's experience with the product to our understanding of the client's resources and priorities, in this case we're exploring phased adoption of some key capabilities like real-time alerts through Tanium Signals.

To Learn More

If you'd like to learn more about how we work to support organizations get the most from their Tanium investments, we'd love to connect. Through years of hands-on experience, working both at Tanium and now as independent consultants, the Chuco team has developed a deep understanding.

So whether you're just starting to work with Tanium, or looking to really push things to the next level, we have experience, insight, and hands ready to assist — be that offering some seasoned advice, working to help execute a specific project, or taking on a role as a virtual member of your internal Tanium team.