CISA 2022 "Top Exploit" List:

How Tanium Can Tame Your Exposure

The Cybersecurity and Infrastructure Security Agency (CISA) has just published its annual list of the most commonly exploited vulnerabilities for 2021.

The report found that in 2021, malicious actors heavily targeted internet-facing systems, such as email servers and virtual private network (VPN) servers, with exploits of newly disclosed vulnerabilities like Log4Shell.

Three of the top 15 exploited vulnerabilities were also routinely exploited in 2020 and demonstrates the continued risk to organizations that fail to patch software in a timely manner or are using software that is no longer supported by a vendor.

The list comprises Common Vulnerabilities and Exposures (CVEs) that are seen actively and frequently exploited in the real world. So for security professionals, if anything should keep you up at night — issues to investigate, check, correct, and then double-check — these should top the list.

Given the high-profile nature of how the CISA report shines a spotlight on these particular attack vectors, time is increasingly of the essence for any organization to get on top of their security housekeeping.

CISA noted that patch management is critical. The abrupt shift to remote and distributed working environments driven by the COVID-19 pandemic is now causing new strain on organizations patching procedures, effectiveness, and compliance levels.

As the world re-orients into hybrid working models, organizations that invest in the right risk strategies will be positioned to address not only the fresh CISA exploit list, but also the ongoing (never ending) security hygiene challenges they face.

Having worked with many clients to address a broad ranges of security issues, we want to share some thoughts, advice, and practical steps to manage your endpoints using Tanium, a leader in converged endpoint management.

Through a Scanner, Darkly

You may have heard the parable about the person hunting for their dropped keys in a dark parking lot at night. A good Samaritan walks up to offer help, but first asks the person why they're only looking under the streetlamp. The reply: "Because that's where the light is."

The point is you need the ability to search everywhere in your environment where vulnerabilities may lurk, not just the places where you "can" search. You need to be able to shine the light everywhere. (And the other point I'd note, that good Samaritans stand ready to help you.)

Translating that to practice effect means increasing visibility across your environment so you can look for exploitable CVEs, reduce your attack surface, and generally mitigate the known (and potentially unknown) risks you face.

And that means implementing a vulnerability risk management strategy for your endpoints. For greatest practical impact, that strategy should include an integrated approach including the right defined processes, designated personnel, and suitable technology to be effective. This is one area Chuco often advises and works with clients to address.

A well-prepared and systematic approach enables organizations to not only address the issues of today, but also build the understanding and capacity to address future issues on the horizon with greater efficiency and speed.

Technology To Light the Way

When it comes to searching for commonly exploited CVEs, organizations have a variety of available scanning technologies to consider.

These include web application security scanners, port scanners, network vulnerability scanners, source code analysis tools, host-based vulnerability scanners, and database security scanners and more.

This is one of several areas where Tanium shines. It provides a host-based vulnerability scanner for your endpoints that effectively and efficiently find not only software vulnerabilities, but also security configurations worth mitigating. Network based scanners can be blocked or limited in functionality by a firewall or can generate much network traffic.

Today, as networks and hosts become more secured, system administrators are less willing to let scanning tools remotely access their machines. Furthermore, host-based scanners have direct access to both the file system on a host and its configuration files and running services. Therefore, this may provide a more complete overview of vulnerabilities.

For Tanium customers that already have the Tanium agent managing their endpoint operations like patching and asset management, it's relatively straight-forward to extend the scope of operations to incorporate the use of the Tanium Comply Module to address these additional security tasks.

For example, organizations can use Tanium Comply to search for all your CVEs to help you identify, categorize, and prioritized your biggest risks. (*See figure 1.*)

It provides the capability to conduct continuous vulnerability and compliance assessments against operating systems, applications, and security policies.

Searches can be scoped not only by most recent CVE, but also by the most routinely exploited issues noted in the recent CISA update.

The Power of an Integrated Approach

As organizations work to make their systematic security measures even more "systematic," Tanium provides integrated capabilities that will scale your efficiency and success:

- Tanium Patch and Deploy empowers organizations to seamlessly transition from identifying vulnerabilities, to launching remediation activities such as patching, third party software updates, or policy and configuration changes to remediate those issues

- Tanium Threat Response enables organization to actively monitor endpoints for suspicious activity and issue event-driven alerts in real time

- And Tanium's reporting capabilities allows organizations to aggregate activity, metrics and results — generating "right scoped" summaries suitable for management eyes

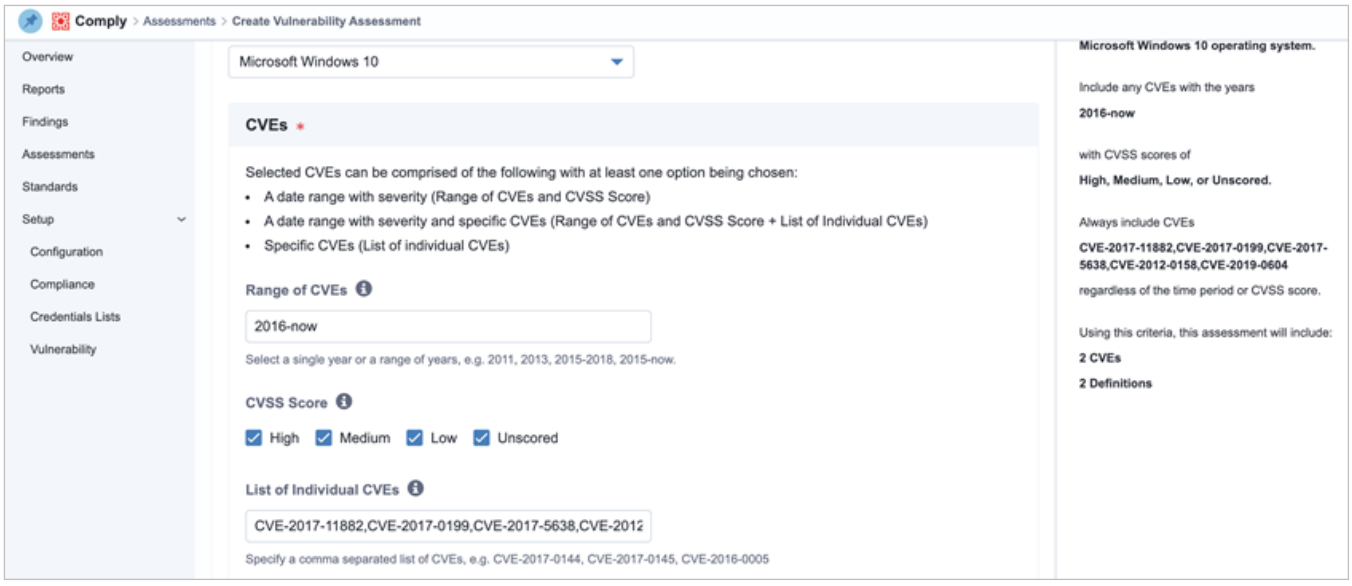

Figure 1

In short, Tanium offers a one-stop, connected security lifecycle management platform, one that can identify vulnerable systems, flag unusual behavior, coordinate patching and other remediation activity, and deliver consolidated reporting suitable for both technical and management audiences. (*See figure 2.*)

A Few Final, Sound Security Sentiments

While the CISA bulletin puts fresh focus on addressing urgent CVEs, I wanted to end with two prudent security reminders.

#1 — Look Backwards as Well as Forwards

While new exploits and alerts warrant urgent attention, it's important to review older CVEs and assess your environment for any lingering unpatched vulnerabilities. In fact, many of the "most exploited" issues are more than two years old.

It's prudent to scan and pen test for both the recent trending vulnerabilities and for older vulnerabilities that are no longer at the top of your email inbox. Remember, hackers will not limit themselves to using the "latest" exploits.

They will take the easiest route, exploiting any open vulnerability of un-patched software and non-compliant systems.

If you're not 100% compliant in patching, it's worth taking a moment to evaluate your practices and consider improvements. It just takes one vulnerable system to lead to a massive breach.

#2 — Stay Nimble as People Return to the Office

In most organizations, the COVID-driven shift to remote working definitely placed new strains on almost every system, person, and process.

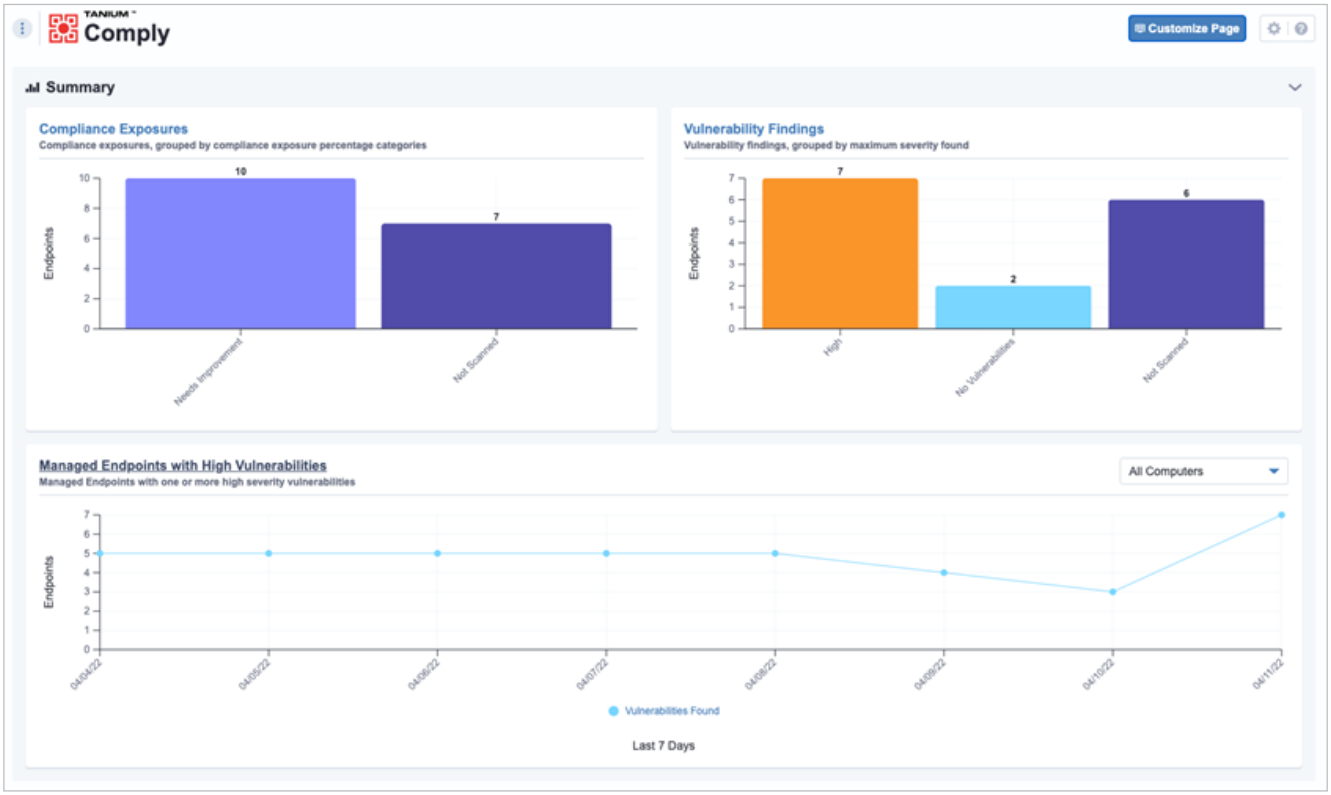

Figure 2

In particular, during the "100% remote" days of the pandemic, attacks on cloud-based emails, remote desktop applications, and unpatched VPN software became much more prevalent, driving security teams to shift priorities and response measures.

Remember that as people return to the office, and increasingly work in multiple locations, it's safe to expect organizations to face greater risks as attack strategies shift and technology teams find it harder to manage the complexity of hybrid networks.

With employees splitting time between the office and off-site location, they're constantly moving in and out of the company network. Oftentimes, off-site employees exercise lax security practices.

For example, they may use work laptops on public networks where they may get exposed to malware. When they return to the corporate network, they may bring that malware back with them.

Taking both recommendations together, now is a good time to review CVEs for the common exploits, not just for 2022, but also for earlier time frames — including exploits used heavily before Covid-19.

The last two years, the most common exploits focused on the "100% remote" based vulnerabilities. As the workforce migrates back to the office, expect new and old "non-remote" exploit types to surface like attacks on unpatched Microsoft and Adobe Flash products.

Cybersecurity crimes continue to increase, and it's vital that organizations are prepared to detect and respond to those security risks. Enacting a proactive endpoint vulnerability management program that includes the right tools, and experienced professionals to use them, will help mitigate significant risk.

Ready to Get (More) Serious about Using Tanium to Tackle Security?

If this has sparked ideas you'd like to explore at your organization, please feel free to get in touch to learn how Chuco can help you respond in the short term to the CISA publication and enhance your security capabilities longer term with Tanium. Our consultants are standing by to help design or extend your response strategy, and put hands on keyboard to help execute, contact info@chuco.com.