Analysis of Company Cybersecurity Vulnerabilities with the Institute for Defense Analyses

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Omer Qasimi is a graduate of George Mason University with a bachelor's degree in cybersecurity engineering. He is currently pursuing a master's degree in Artificial Intelligence. His academic background, combined with hands-on internship experience, has provided him with a strong foundation in cybersecurity principles, secure system design, and data-driven technologies. His interests include applying artificial intelligence to enhance security, automation, and real-world problem-solving.

Bella Tran is a student at George Mason University graduating with a bachelor's degree in information technology and concentrating in Cybersecurity. Her hands-on experience through projects and internships has strengthened her skills in problem-solving, critical thinking, and applying technology to real-world challenges. She is passionate about building a long-term career in both IT & Cyber, where she can further apply and develop her professional skills.

----- ***Industry Participant / Mentor*** -----

Christopher Murphy
Enterprise IT Operations Manager
Institute for Defense Analyses

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
FWI Corporate Partner Faculty Fellow
Assistant Dean, Centers of Excellence
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

During our PREP project, we supported IDA's vulnerability management efforts on its unclassified network. The main goal of the project was to review vulnerability scan results and help reduce security risks. We used Tenable Security Center to analyze identified vulnerabilities and determine which issues needed to be addressed first.
Our work focused on mitigating these vulnerabilities by reviewing findings, recommending fixes, and tracking progress. We used Excel to document vulnerabilities, record mitigation efforts, and maintain organized records throughout the project. This process made security issues easier to track and contributed to improving IDA's overall security posture.

Business Challenge

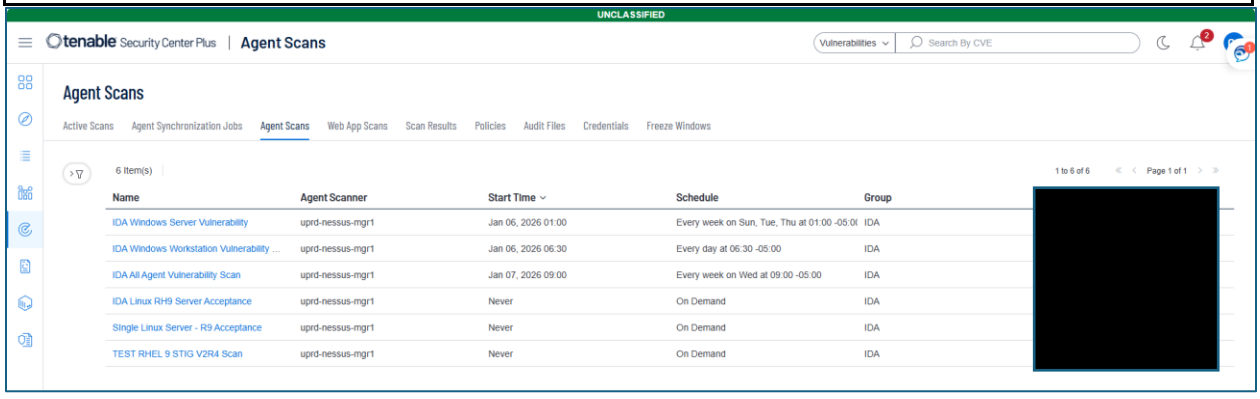
IDA was facing a growing number of vulnerabilities across its unclassified systems and workstations. Many of these vulnerabilities were high or critical, creating potential risks to the security and integrity of their systems and data. A major challenge was that, without an automated system, it was difficult to notify the appropriate users about these vulnerabilities in a timely manner. With so many systems affected, manually informing each user was inefficient and prone to delays. Our team stepped in to help streamline this process by reviewing vulnerability findings and assisting in notifying users so that remediation actions could be taken more quickly and effectively.

Activities Done to Address the Business Challenge

To reduce security risks in IDA, our team took a hands-on approach to identify weaknesses, apply fixes, and improve how issues are handled over time. By working together as one team, we ensured that problems were addressed efficiently and that better practices were put in place to prevent future issues.

- **Analyzing Scans:** We regularly reviewed and monitored new scans in the Agent Scans section to check scheduled and on-demand scans performed by the cybersecurity team. These scans helped us know the upcoming scheduled scans performed on systems.

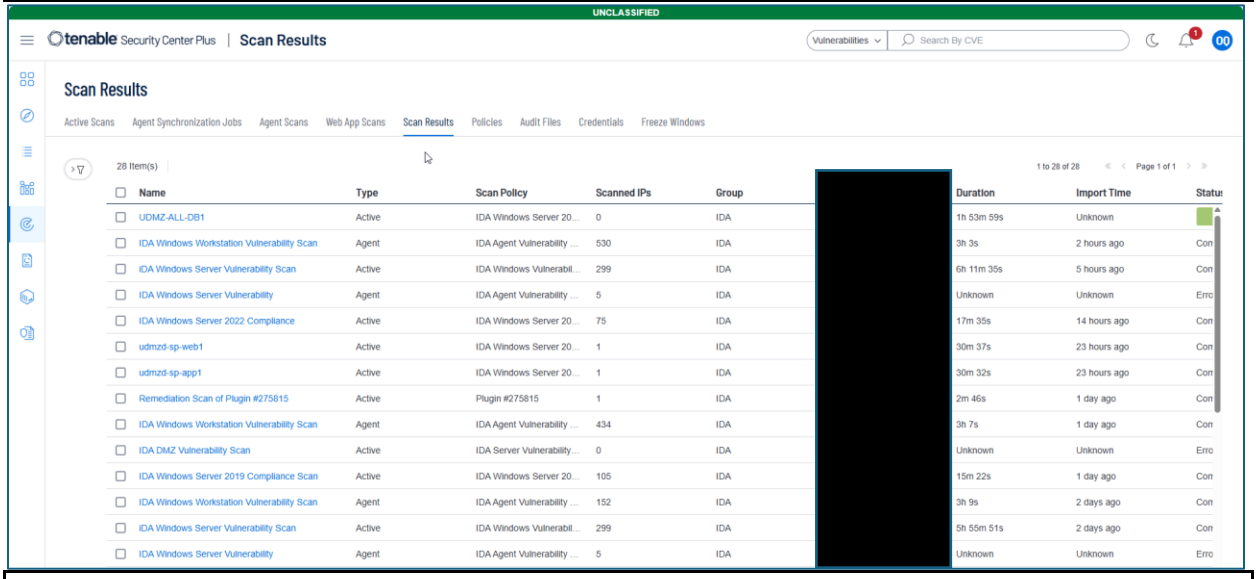
Tenable Agent Scan List



This screenshot displays scheduled and on-demand scans configured by the cybersecurity team.

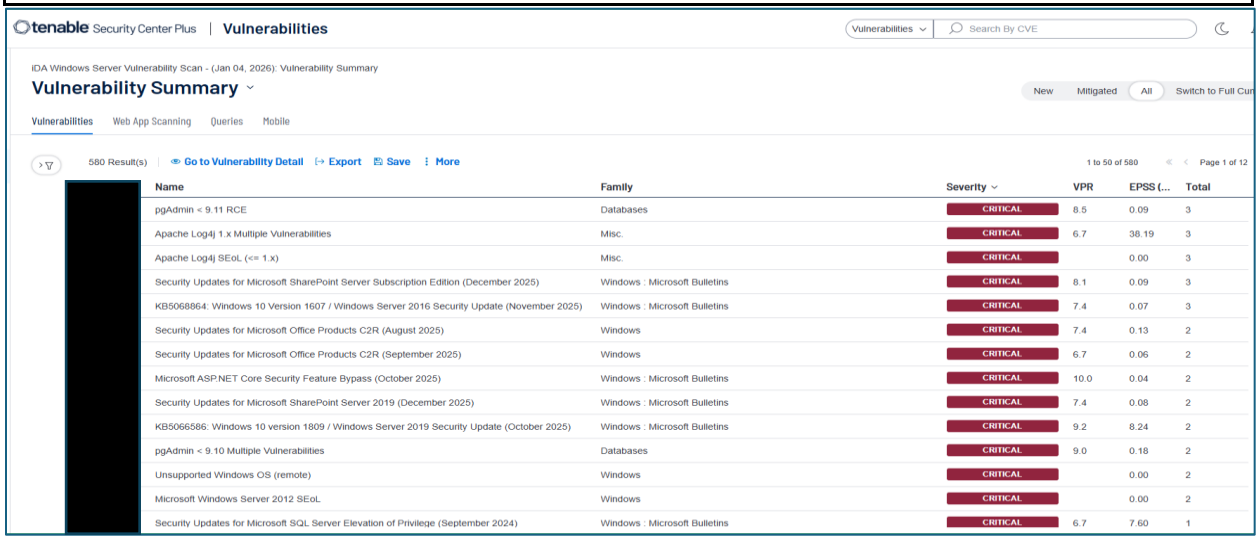
- **Scan Results Review:** We reviewed and analyzed scan results in the Scan Results section to track completed vulnerability and compliance scans performed by the cybersecurity team. These results provided visibility into scanned systems, scan duration, and identified vulnerabilities, enabling our team to assess security posture and prioritize remediation efforts accordingly.

Scan Results Overview



This screenshot displays the scan results from scheduled and on-demand vulnerability and compliance scans conducted by the cybersecurity team, providing visibility into scan status, duration, and scanned systems.

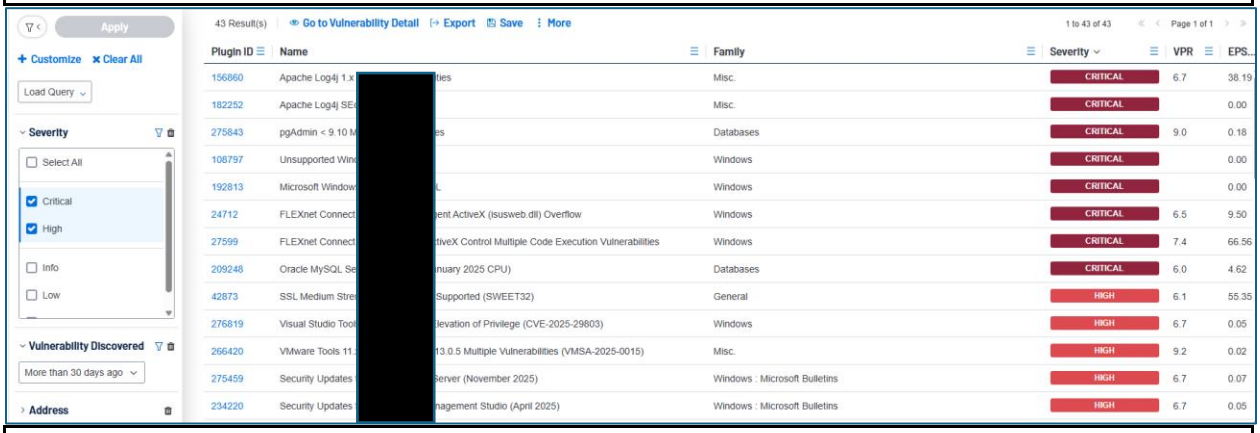
Vulnerability Summary Details



This screenshot shows the first screen of vulnerability results from a Tenable Windows Server scan.

- **Targeted Severity Filtering:** We filtered out lower-priority vulnerabilities and prioritized the critical and high-impact ones.

Filtering on Tenable



This screenshot shows the filtered vulnerability list from our Tenable dashboard, focusing on critical and high-severity that are more than 30 days ago.

- **Vulnerability Detailed analysis:** We conducted a detailed analysis of identified vulnerabilities by reviewing individual vulnerability records in the Vulnerability Detail List. This view provided in-depth information, including severity level, affected hosts, discovery timeline, vulnerability description, and recommended remediation steps. This detailed analysis also allowed us to further research each vulnerability by referencing the CVE database for more in-depth technical information and leveraging the MITRE ATT&CK framework to understand potential attacker tactics, techniques, and procedures. By analyzing these details, our team was able to better assess risk impact, prioritize high-severity findings, and apply appropriate security updates to effectively mitigate the identified vulnerabilities.

Before Remediation

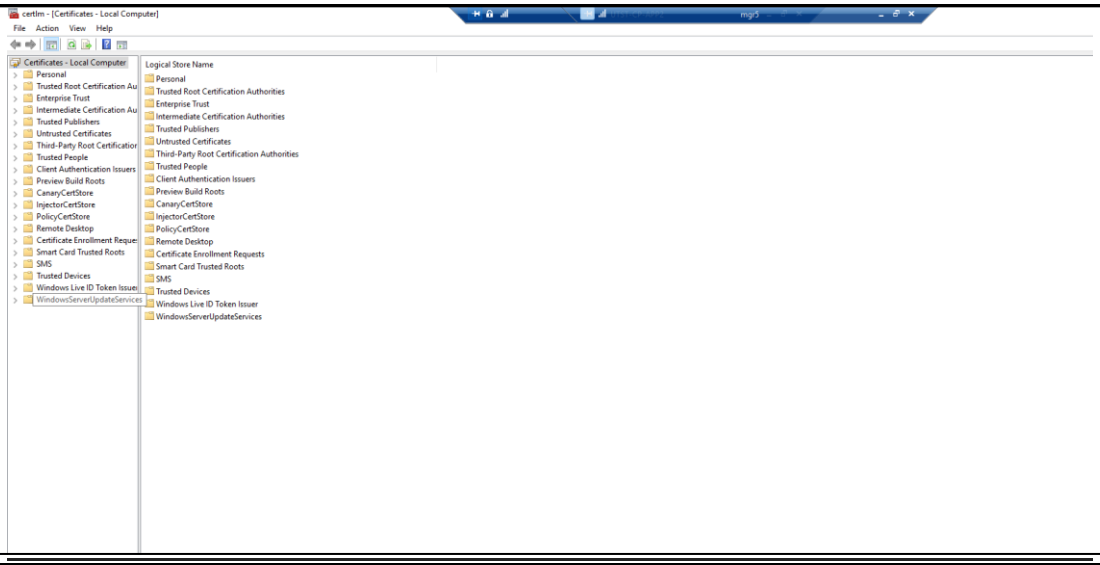
133 Result(s) | Go to Vulnerability Detail | Export | Save | More — 1 to 50 of 133 — Page 1 of 3

Plugin ID	Plugin Name	Family	Severity	VPR	EPS...	IP Address	ACR	AES	[redacted]	DNS
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.11.0.6	5	531		stpl-p
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.30.106	5	408		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.45.201	5	0		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.168.25	5	529		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.30.98	5	0		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.12.9	5	413		msdt(
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.30.87	5	418		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.30.87	5	418		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.31.133	5	408		udev-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.0.74	5	138		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.0.30.41	5	474		reme
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.11.60.22	5	507		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.11.60.22	5	507		uprd-
57582	SSL Self-Signed Certificate	General	MEDIUM		0.00	10.11.60.22	5	507		uprd-

This screenshot shows a vulnerability scan summary listing 133 instances of **SSL Self-Signed Certificate** issues across various servers.

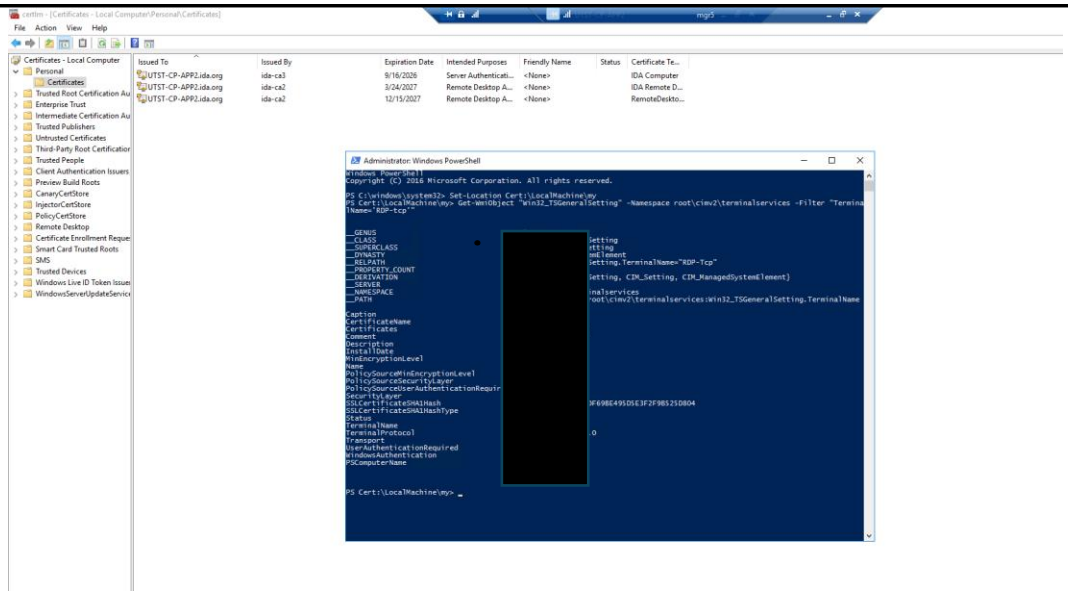
- **Remediation Progress:** To remediate identified vulnerabilities, our team applied multiple remediation approaches based on the nature of each issue. One example is the remediation of SSL self-signed certificate vulnerabilities, for which the step-by-step remediation process is shown below.

Certlm.msc Certification Location



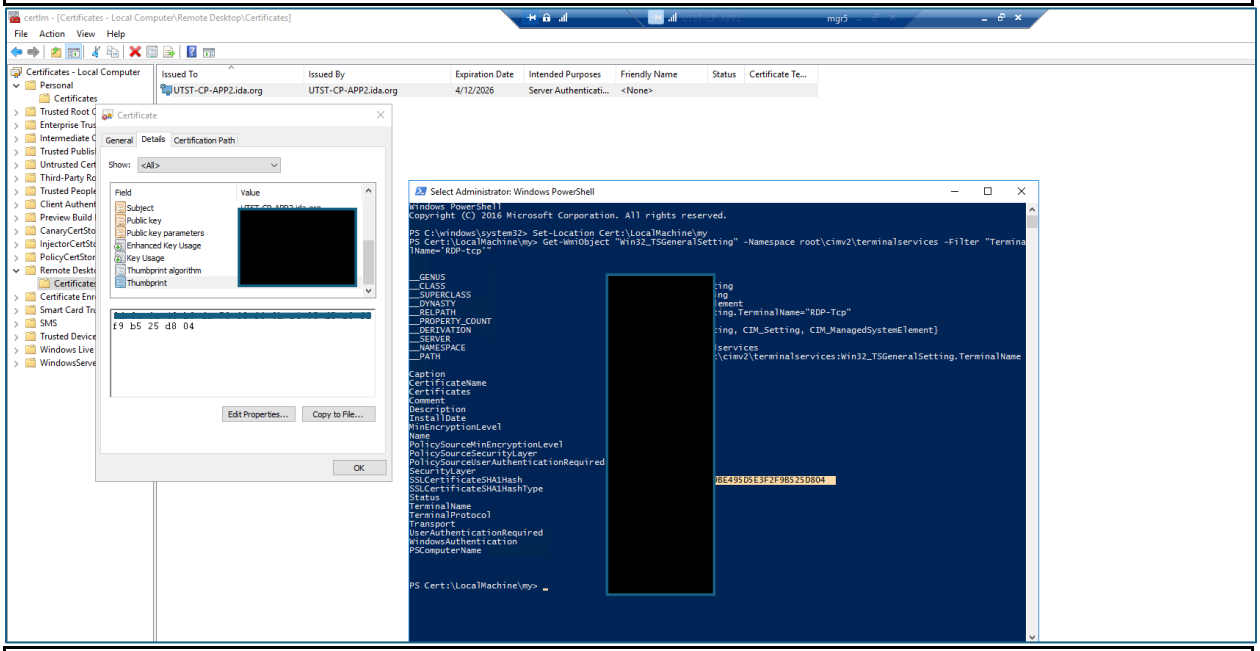
This screenshot shows the locations of different certificates on the device. We needed to locate the certification location for confirmation.

Certificate Confirmation



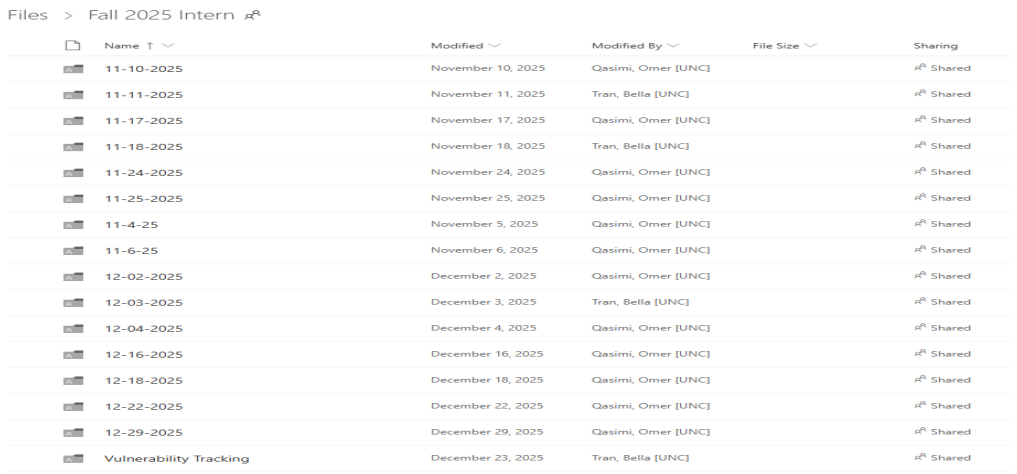
We ran these Powershell Commands using admin privileges to check which certificate is in use for the specific server

Certificate Confirmation with Thumbprint hash



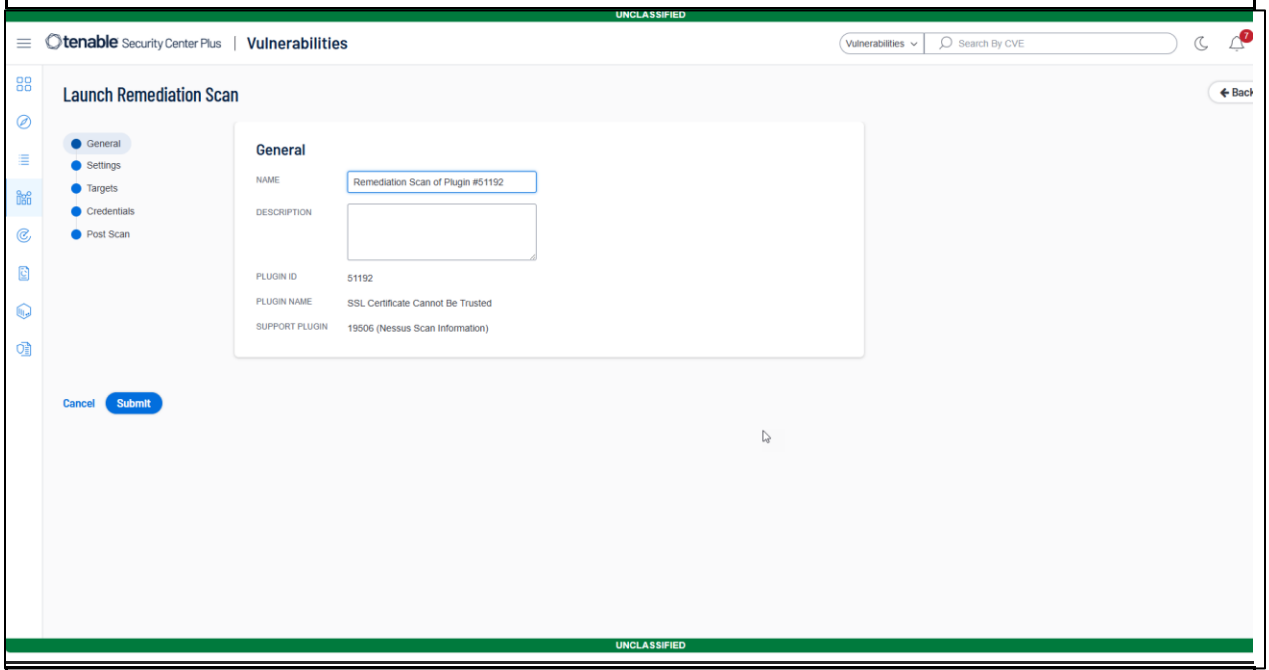
The Certificate details confirms the location of the exact certificate the system is currently using by matching the thumbprint hash with the finding on the Powershell

Updating server's SSL Certificate



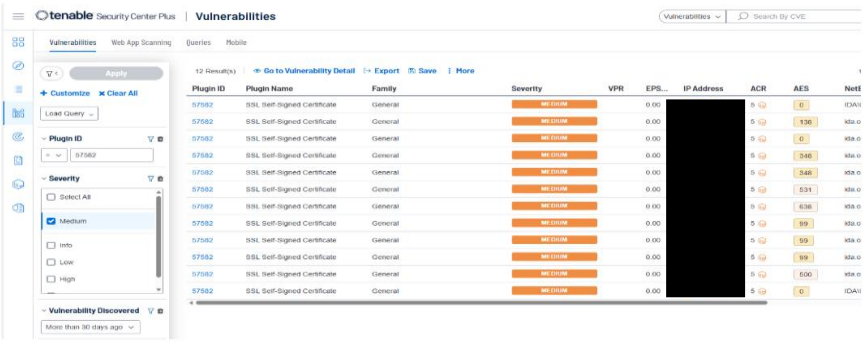
To update the SSL certificate, we executed the commands shown in the PowerShell screenshot. To verify the update was successful we then compared the updated certificate thumbprint displayed in PowerShell with the certificate hash on the device to confirm successful installation.

Remediation Scan



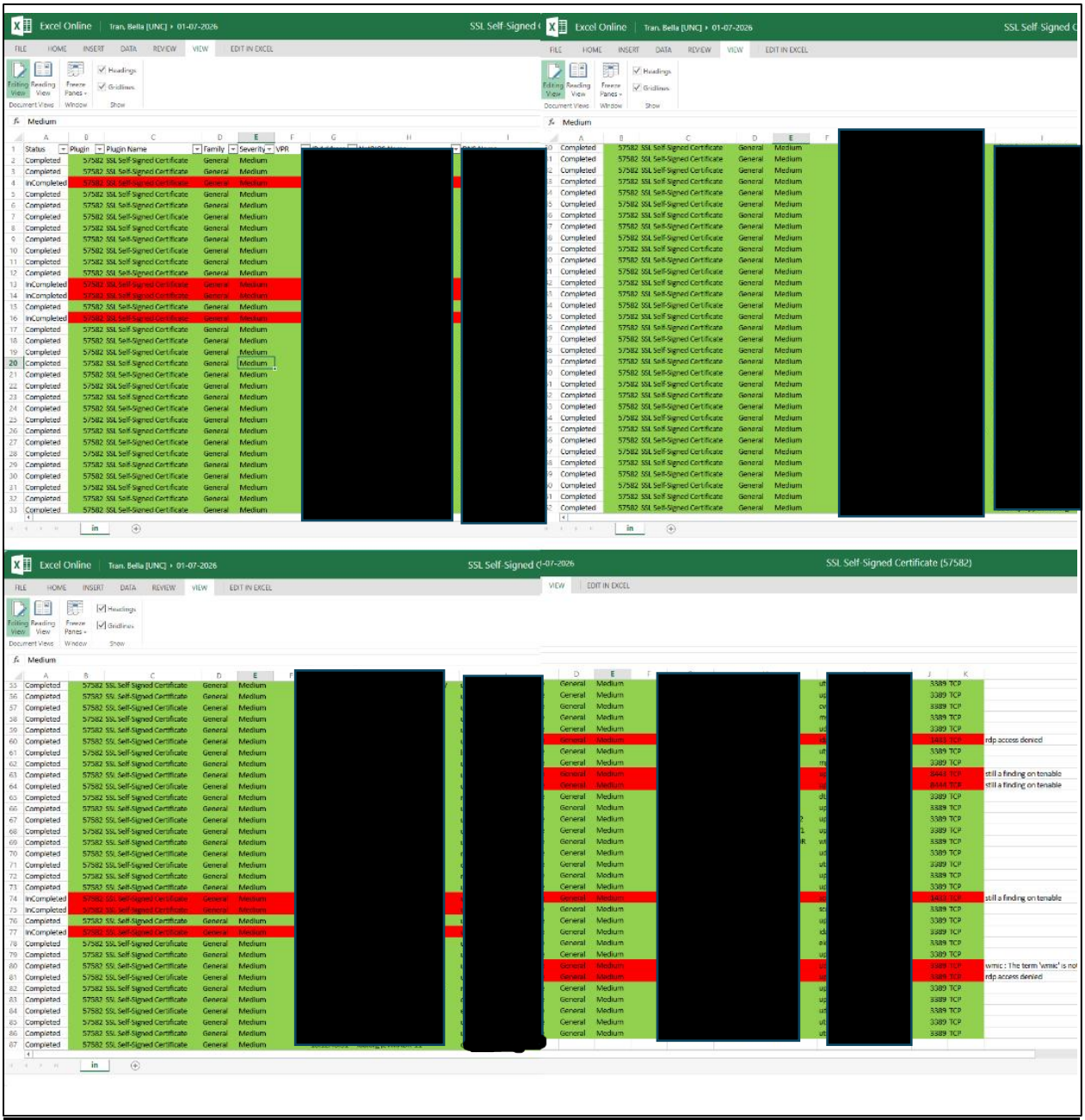
After successfully remediating the server, we ran a remediation scan to verify that the remediation process was successful.

After Remediation



DNS	MAC Address	Port	Protocol	Repository
uprd-adfs-idm2.ida.org		3389	TCP	Individual Scan
sccm-test01.ida.org		1433	TCP	Individual Scan
sccm-test03.ida.org		1433	TCP	Individual Scan
utst-epo-fips1.ida.org		8443	TCP	Individual Scan
utst-epo-fips1.ida.org		8444	TCP	Individual Scan
uprd-rds-cb-01.ida.org		443	TCP	Individual Scan
idapdms01.ida.org		1433	TCP	Individual Scan

This screenshot shows the reduced number of remaining SSL self-signed certificate findings after remediation efforts. Our team successfully resolved **over 130 vulnerabilities**, as reflected in the scan results. The remaining findings are associated with different ports that were outside the scope of our remediation focus



Post-remediation documentation of SSL self-signed certificate findings, showing all resolved items recorded in Excel following the successful remediation of over **130 vulnerabilities** across affected servers

Results & Metrics

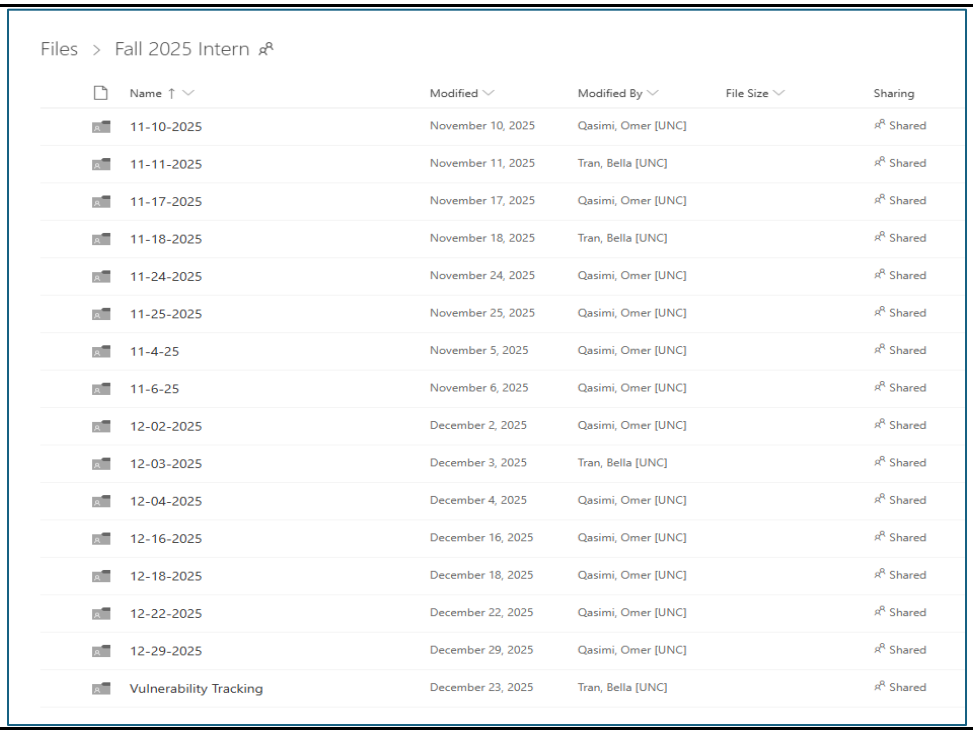
- **Results Tracking**: For each new Windows Server vulnerability scan, we created folders to track the vulnerabilities we had worked on.

Vulnerability Tracking and Remediation Summary

Total
='Windows Defender #135718'!J2 + 'Microsoft Defender #127910'!G2 + 'Dell Client BIOS #192946'!D2 + 'Microsoft SQL Server #207065'!E2 +'Windows MSRT #169783'!E2 + 'SWEET32 #42873'!E2 + 'Microsoft Azure Data #192147'!E2 + 'R Programming Language #195217'!E2 + 'Microsoft SQL Server #241544'!E2 + 'WinVerifyTrust #166555'!I2 + 'Visual Studio Tools #276819'!E2 + 'Microsoft SQL Server #275459'!E2 + 'Wireshark #275815'!E2 + 'SSL Certificate #57582'!E2 + 'SSL Certificate #51192'!E2

This screenshot shows the Excel tracking sheet used to document vulnerability findings and their corresponding Tenable plugin IDs. It represents the full set of vulnerabilities our team worked on throughout the project, totaling **340+ remediations**. This tracking approach helped us organize findings, monitor remediation progress, and verify successful resolution across systems.

Tracking and Collaborating using SharePoint

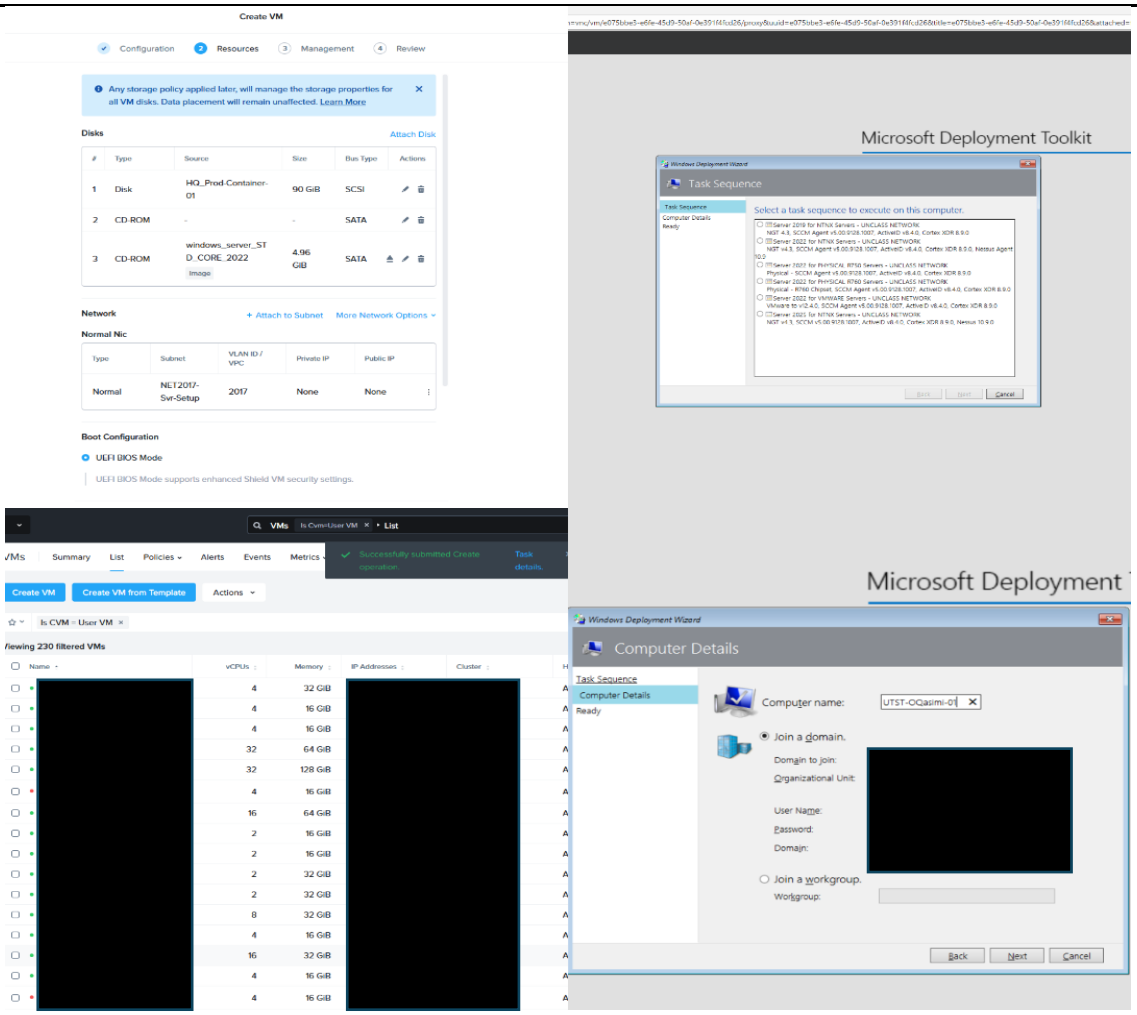


This screenshot shows how our team organized and shared folders to track vulnerabilities from each Windows Server scan.

Skills Development & Team Learning

- **Building Virtual Server:** Setting up the Nutanix virtual machine gave our team practical, hands-on experience with server provisioning and infrastructure in an enterprise environment. We worked on allocating system resources, configuring networking, and deploying an operating system using Microsoft Deployment Toolkit (MDT), ensuring the server was fully integrated into the environment. This experience helped us understand how virtual servers are built and reinforced the importance of consistent configuration and teamwork when deploying reliable systems for everyday use.

Building Server Using Nutanix



These screenshots show how our team built and configured a server, including setting up the virtual machine, allocating system resources, configuring network settings, and selecting boot options. It also highlights the use of MDT to install the operating system, choose the appropriate task sequence, name the server, and join it to the domain. This process helped ensure new servers were set up consistently and ready for use in the environment.

Windows Welcome Screen Created Server

This screenshot shows the successful completion of the Nutanix server build, displaying the welcome screen. The server is fully configured and ready for normal day-to-day use without any issues.

Results & The Positive Impact

Our team helped improve the vulnerability management process by reviewing older findings and identifying the appropriate application and asset owners to contact for updates. By reaching out and following up on these findings, we helped reduce the number of unresolved issues.

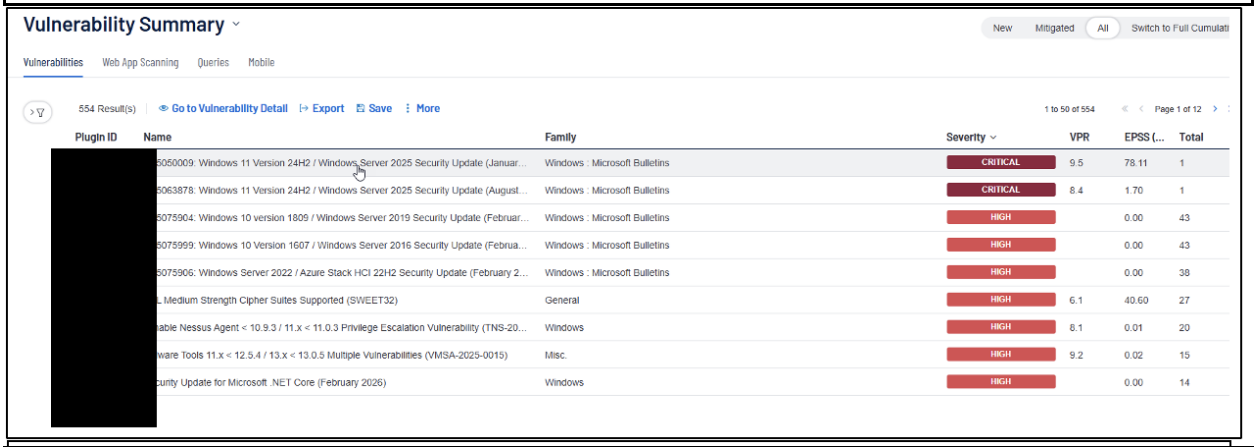
In addition to that, we verified the remediation status of vulnerabilities by consistently reviewing new scan results to confirm whether patches were successfully applied. For vulnerabilities that showed up again on the recent scans, even after mitigation efforts, we worked collaboratively to identify the root causes and provided clearer explanations to ensure users or system owners understood the severity and the recommended actions to keep their systems safe.

Phase II: Continued Vulnerability Remediation & Progress Update

- Following the completion of the initial remediation effort, our team continued vulnerability management activities as part of Phase II. The focus was to further reduce aging vulnerabilities, validate prior remediations, and address newly discovered high- and critical-severity findings. Our team reviewed affected hosts, contacting asset owners, and validating remediation efforts through follow-up scans. We were able to close a significant portion of previously unresolved findings. Particular attention was

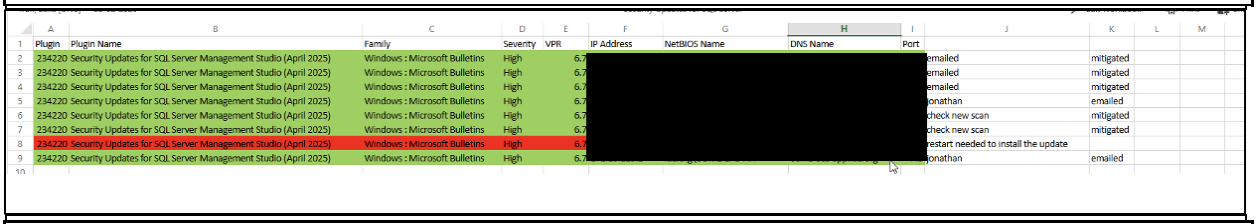
given to recurring vulnerabilities affecting multiple servers, ensuring that remediation was consistently applied across all impacted assets rather than resolved on a single system. This structured approach improved remediation efficiency and reduced the risk of recurring findings in subsequent scans.

Ongoing Scan Monitoring & Prioritization



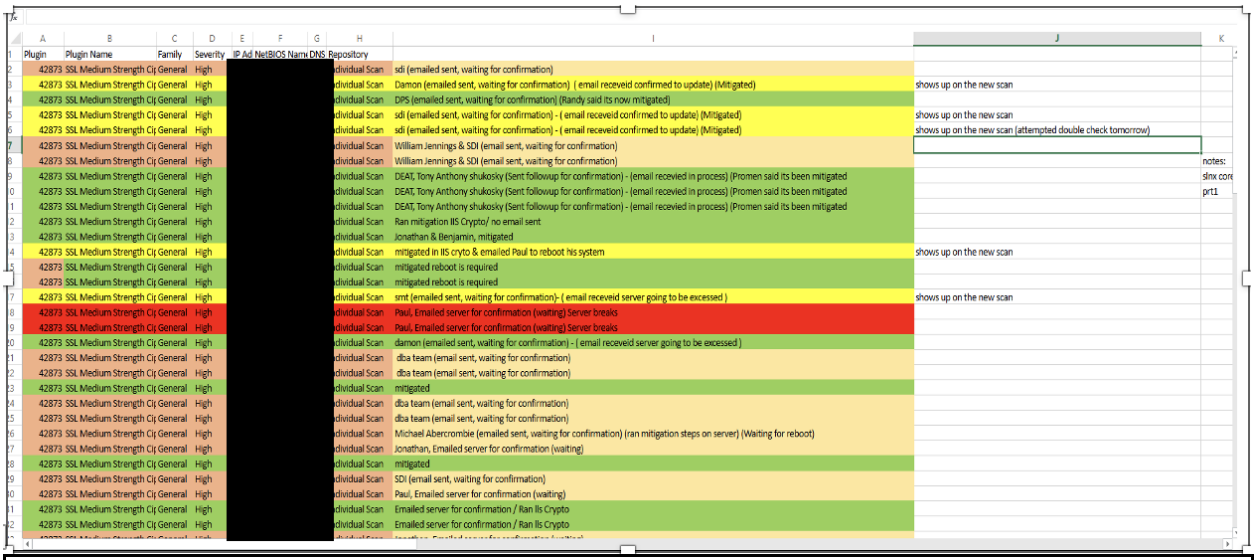
This screenshot displays the Tenable Vulnerability Summary dashboard highlighting active vulnerabilities categorized by severity. The view emphasizes critical and high-severity findings, including Microsoft security update bulletins and configuration-related vulnerabilities, which were prioritized for remediation during Phase II to reduce overall risk exposure.

SQL Server Vulnerability Tracking and Remediation Status



This screenshot displays the Excel-based vulnerability tracking sheet used to monitor high-severity findings across affected systems. The highlighted entries reflect remediation progress, including mitigated vulnerabilities, systems pending updates, and follow-up validation efforts. This structured tracking approach supported the reduction of aging and high-severity vulnerabilities during Phase II.

Significant Progress in Remediating SSL Medium Strength Cipher Suites



Plugin	Plugin Name	Family	Severity	IP Ad	NetBIOS Name	DNS	Repository			
42873	SSL Medium Strength Ci	General	High	[redacted]			dividual Scan	sdi (emailed sent, waiting for confirmation)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Damon (emailed sent, waiting for confirmation) (email receveid confirmed to update) (Mitigated)	shows up on the new scan	
42873	SSL Medium Strength Ci	General	High				dividual Scan	DPS (emailed sent, waiting for confirmation) (Randy said its now mitigated)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	sdi (emailed sent, waiting for confirmation) - (email receveid confirmed to update) (Mitigated)	shows up on the new scan	
42873	SSL Medium Strength Ci	General	High				dividual Scan	sdi (emailed sent, waiting for confirmation) - (email receveid confirmed to update) (Mitigated)	shows up on the new scan (attempted double check tomorrow)	
42873	SSL Medium Strength Ci	General	High				dividual Scan	William Jennings & SDI (email sent, waiting for confirmation)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	William Jennings & SDI (email sent, waiting for confirmation)		notes:
42873	SSL Medium Strength Ci	General	High				dividual Scan	DEAT, Tony Anthony shukosky (Sent followup for confirmation) - (email recevied in process) (Promen said its been mitigated		slnx cor
42873	SSL Medium Strength Ci	General	High				dividual Scan	DEAT, Tony Anthony shukosky (Sent followup for confirmation) - (email recevied in process) (Promen said its been mitigated		prt1
42873	SSL Medium Strength Ci	General	High				dividual Scan	DEAT, Tony Anthony shukosky (Sent followup for confirmation) - (email recevied in process) (Promen said its been mitigated		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Ran mitigation IIS Crypto/ no email sent		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Jonathan & Benjamin, mitigated		
42873	SSL Medium Strength Ci	General	High				dividual Scan	mitigated in IIS cryto & emailed Paul to reboot his system	shows up on the new scan	
42873	SSL Medium Strength Ci	General	High				dividual Scan	mitigated reboot is required		
42873	SSL Medium Strength Ci	General	High				dividual Scan	mitigated reboot is required		
42873	SSL Medium Strength Ci	General	High				dividual Scan	smt (emailed sent, waiting for confirmation)- (email receveid server going to be excessed)	shows up on the new scan	
42873	SSL Medium Strength Ci	General	High				dividual Scan	Paul, Emailed server for confirmation (waiting) Server breaks		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Paul, Emailed server for confirmation (waiting) Server breaks		
42873	SSL Medium Strength Ci	General	High				dividual Scan	damon (emailed sent, waiting for confirmation) - (email receveid server going to be excessed)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	dba team (email sent, waiting for confirmation)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	dba team (email sent, waiting for confirmation)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	mitigated		
42873	SSL Medium Strength Ci	General	High				dividual Scan	dba team (email sent, waiting for confirmation)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	dba team (email sent, waiting for confirmation)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Michael Abercrombie (emailed sent, waiting for confirmation) (ran mitigation steps on server) (Waiting for reboot)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Jonathan, Emailed server for confirmation (waiting)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	mitigated		
42873	SSL Medium Strength Ci	General	High				dividual Scan	SDI (email sent, waiting for confirmation)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Paul, Emailed server for confirmation (waiting)		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Emailed server for confirmation / Ran Ils Crypto		
42873	SSL Medium Strength Ci	General	High				dividual Scan	Emailed server for confirmation / Ran Ils Crypto		

This screenshot displays the tracking and remediation status of the SSL Medium Strength Cipher Suites (SWEET32) vulnerability across multiple systems. This vulnerability remains one of the key high-severity findings currently being addressed. The majority of affected systems have been successfully mitigated through configuration updates and validation scans. The remaining instances are actively being monitored, with follow-ups sent to respective server owners and confirmations pending to complete remediation. This structured tracking approach ensures continued progress toward full resolution while maintaining visibility into outstanding items.

Conclusion

This project supported IDA's vulnerability management efforts by reviewing scan results, prioritizing high- and critical-severity findings, and assisting with remediation across the unclassified network. Using the Tenable Security Center along with structured tracking in Excel and SharePoint, we as a team helped reduce a significant number of aging and unresolved vulnerabilities and continued building on that progress in Phase II.

Across both phases of the engagement, our team assisted in the remediation and validation of **over 340 vulnerabilities**, while also advancing additional high-severity findings and confirming previously resolved issues through follow-up scans. Our focused efforts on SSL-related vulnerabilities and other recurring high-impact findings led to measurable improvements in the organization's overall security posture. This experience not only strengthened IDA's vulnerability management process but also gave us valuable hands-on exposure to real-world enterprise cybersecurity operations and collaborative remediation efforts.

PREP Student Reflection

Omer Qasimi - This fall 2025 PREP internship gave me hands-on experience in vulnerability management, endpoint assessment, and remediation in a real-world enterprise environment. I worked with tools like Tenable and Active Directory to find, track, and fix vulnerabilities, getting

a clear picture of how security teams prioritize and protect critical systems. With my team, I helped close nearly 340 vulnerabilities and made sure systems were properly configured and secure. This experience also gave me a better understanding of how virtual servers, endpoints, and networks work together, and showed me how important teamwork and attention to detail are in cybersecurity operations. Applying my background in AI and digital systems helped me approach problems more efficiently and analytically. Overall, this internship strengthened my technical skills, expanded my practical knowledge, and reinforced my goal of contributing effectively to cybersecurity.

Bella Tran - This PREP internship has provided me with a valuable opportunity to learn and work with various tools such as SharePoint, Excel, Nutanix, Active Directory, and mainly Tenable Security Center Plus. I gained a deeper understanding of how vulnerabilities are identified, tracked, and mitigated, as well as what it is like to collaborate within a professional team environment. Throughout the program, our team reviewed scan results, focused on older vulnerabilities, and identified the appropriate users to notify them for remediation. This experience strengthened my attention to detail, communication skills, and ability to work through real-world security challenges while developing both non-technical and technical skills relevant to my future career. Overall, this project served as a steppingstone toward my career in both IT and cybersecurity and provided practical experience that I will continue to build on as I develop my technical and professional skills.