Vulnerability Assessment
Executive Report

Virginia Bankers Association
Glen Allen, Virginia

Performed
3/29/2024

Prepared by:
SBS CyberSecurity's
Network Security Team

The information contained in this report was derived from proprietary data provided by Virginia Bankers Association - Glen Allen, Virginia

Purpose:

Vulnerability Assessments are an important part of creating a secure information technology (IT) environment and identifying the risks that are currently facing a Client. Vulnerability Assessment is the process of locating and reporting vulnerabilities affecting the confidentiality, integrity, and availability of information systems. As part of a strong information security program, a Vulnerability Assessment helps to reduce the levels of reputational, strategic, and financial risk to a Client. This Executive Report presents an overview of these findings.

Scope:

This Vulnerability Assessment was performed at Virginia Bankers Association of Glen Allen, Virginia. Findings from the assessment have been compared to Banks of similar size, using an industry-leading network analysis tool. This assessment evaluated vulnerabilities on all devices properly connected to the network(s) and powered on at the time of the assessment.

Reporting:

The findings documented in this report are grouped into the following three sections:

Vulnerability Assessment Overview: Demonstrates an overview of the results from the Vulnerability Assessment performed on 3/29/2024.

Peer Comparison: Shows how comparative data from the Vulnerability Assessment performed at Virginia Bankers Association compares to Vulnerability Assessment data gathered by SBS CyberSecurity from Banks of a similar size over the past year.

Vulnerability Assessment History: Demonstrates to management the overall effectiveness of Virginia Bankers Association's Patch Management Program and vulnerability mitigation process from past Vulnerability Assessments performed by SBS CyberSecurity.

Findings:

SBS CyberSecurity's Vulnerability Assessment process, completed on 3/29/2024, identified a total of 28 high priority vulnerabilities within 13 different programs on 26 of Virginia Bankers Association systems. Out of the 28 vulnerabilities, there were found to be 17 unique vulnerabilities propagated across Virginia Bankers Association's network. For more detailed information about these findings, please reference the Vulnerability Assessment Report.

About this Assessment:

This Vulnerability Assessment was performed at the request of Virginia Bankers Association in Glen Allen, Virginia on 3/29/2024, by the Network Security Team for SBS CyberSecurity, LLC of Madison, SD. The Network Security Team consists of individuals who hold the following industry recognized certifications: Certified Penetration Tester (CPT), Certified Ethical Hacker (CEH) and Security+. This assessment was overseen by Justin Curtner, Information Technology Auditor for SBS CyberSecurity, LLC of Madison, SD. Justin has 8 years of experience in business operations and security. Justin has received his Bachelor of Science in Business Administration from Arkansas State University and is a Certified Community Banking Security Professional (CCBSP).

SBS CyberSecurity (SBS) is a premier cybersecurity consulting and audit firm. Since 2004, SBS has been dedicated to assisting organizations with the implementation of valuable risk management programs and to mitigating cybersecurity risks. The company has provided cybersecurity solutions to over 1,300 organizations across the United States and abroad, including financial Clients ranging in asset size from $12 million to over $20 billion. SBS delivers unique, turnkey solutions tailored to each client's needs, including cybersecurity risk management software, consulting services, network security, IT audit, and education. SBS CyberSecurity empowers customers to make more informed security decisions and trust the safety of their data.

Vulnerability Assessment Overview

Top Software Threats

The following table shows the top programs based on their perceived threat to the network. A vulnerability's threat is based on its occurred impact and probability of being exploited. The table below shows the represented threat the top programs present to Virginia Bankers Association based on the overall threat score as well as the number of vulnerabilities for each of the programs. If the following programs are patched with the recommended fixes, Virginia Bankers Association will mitigate 69% of the network's perceived threat.

Top Software Threats

Program Name	Total Vulnerabilities on Network	Represented Threat to Network
Apache Log4j	4	17%
Microsoft 3D Viewer	4	15%
.NET Framework	3	13%
Windows 10 1607 and Server 2016	3	13%
Microsoft Windows	3	11%

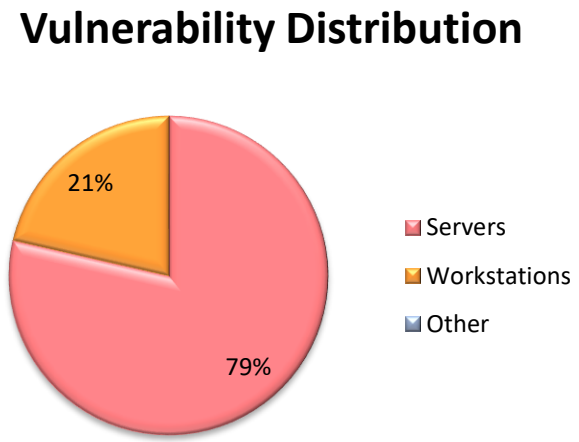
Top Systems by Inherent Risk

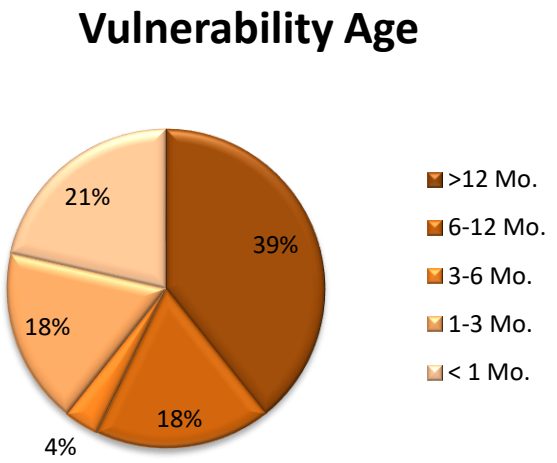
The following table shows the top systems based on their Inherent Risk to the network. Inherent Risk Scores are calculated based on the Total Threat and the system's Protection Profile. The table details the total Vulnerabilities found on the system, the calculated Protection Profile based on scan information, and the represented Total Threat Score.

Top Systems by Inherent Risk

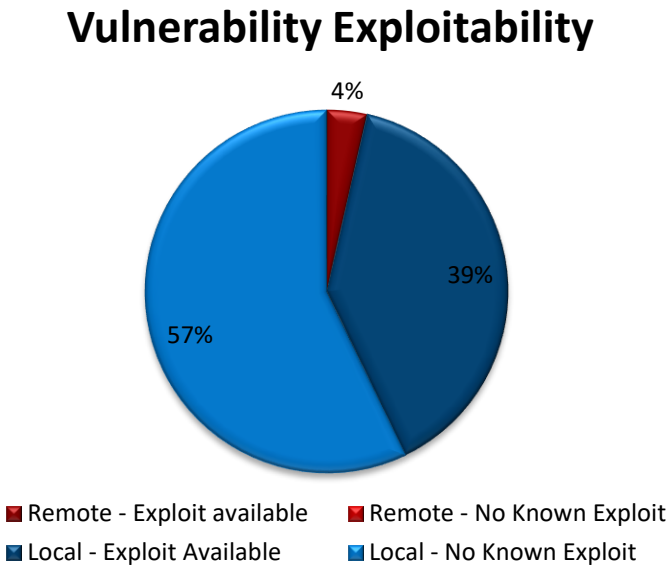
System Name / IP	Total Vulnerabilities on System	Protection Profile	Total Threat Score
VBASQL / 172.20.4.10	7	10	65.2
VBADC / 172.20.4.14	3	10	27.6
VBAFAS / 172.20.4.13	3	10	27.2
VBANPS / 172.20.4.18	3	10	20.0
VBAFS / 172.20.4.19	3	10	20.0

Vulnerability Distribution
The following charts indicate the distribution of vulnerabilities across servers, workstations, and other devices attached to the network. In addition, the amount of time between the date of the vulnerability identification by the security community and the date this Vulnerability Assessment was conducted is represented (in months) by the Vulnerability Age chart.





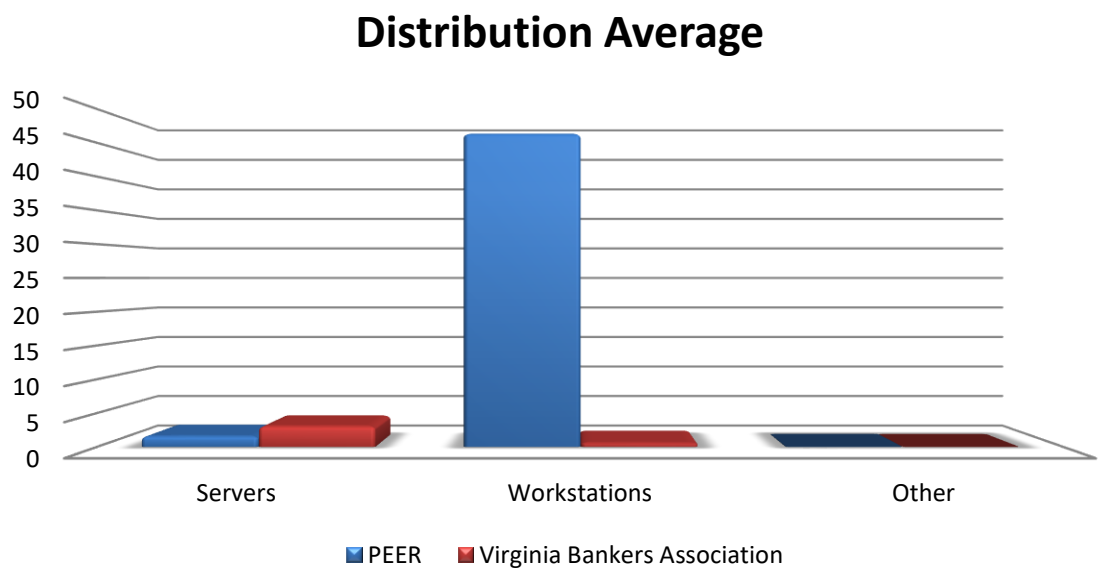
Severity and Quality
The Vulnerability Exploitability chart shows the percentage of vulnerabilities found that could be exploited locally (an attacker would need access to the local host or require interaction from the user to exploit) and remotely (an attacker would need access to the local network to exploit) and of those findings, which currently have a publicly known exploit and which currently do not have a publicly known exploit.



Peer Comparison

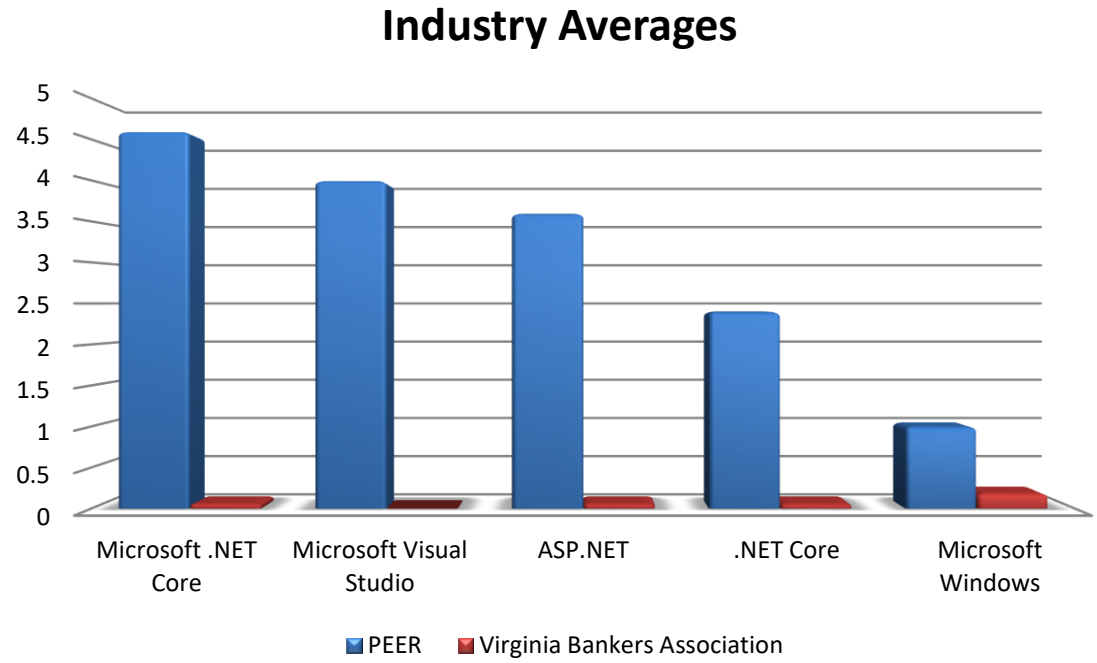
Industry Average Distribution

The Distribution Average chart compares the average number of vulnerabilities on servers, workstations, and other devices attached to the network to Banks of similar size.



Industry Patch Management Trends

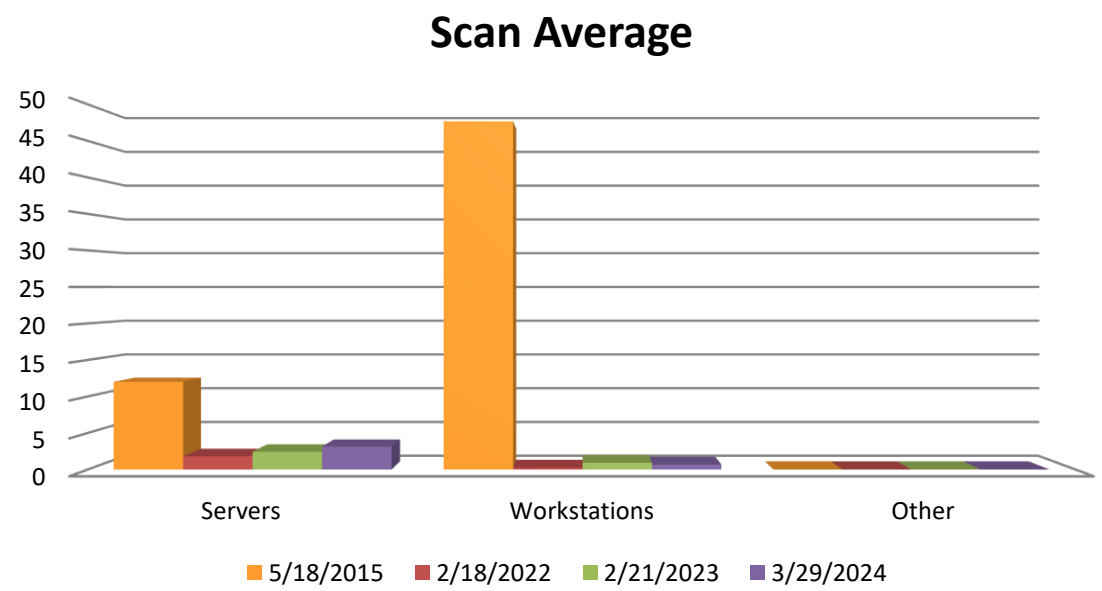
The Industry Averages chart compares the percentage of the total vulnerabilities that the 5 most common programs (in the past year) have in other Banks of similar size to Virginia Bankers Association's network.



Vulnerability Assessment History

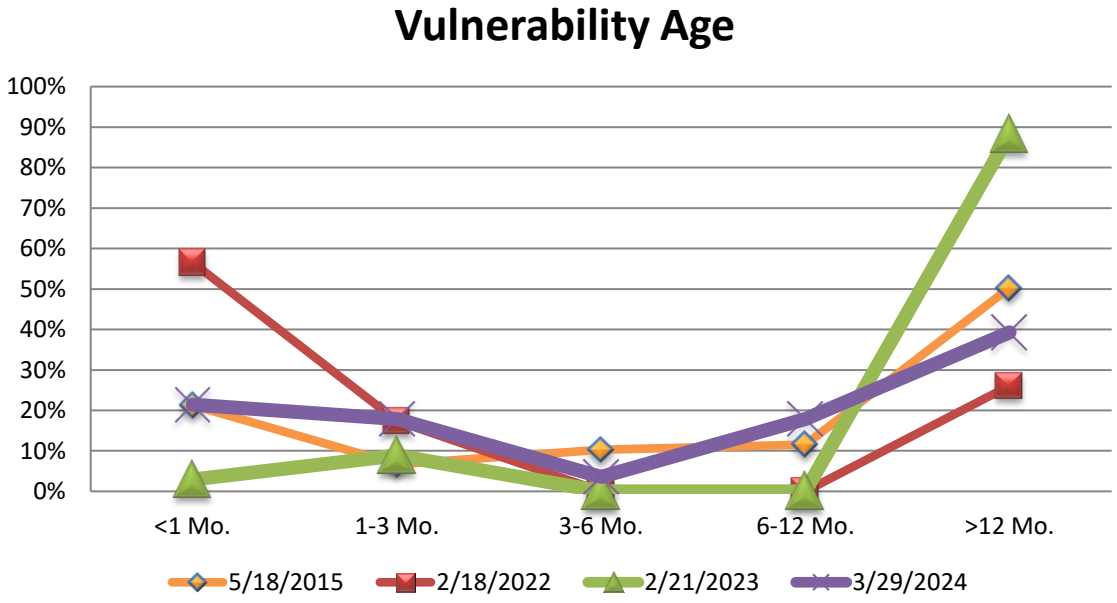
Vulnerability Distribution

The following chart indicates the distribution of vulnerabilities across servers, workstations and other devices attached to the network as compared to previous Vulnerability Assessments performed by SBS CyberSecurity.



Vulnerability Age

This chart demonstrates the ages of vulnerabilities found as compared to previous Vulnerability Assessments performed by SBS CyberSecurity and indicates any change in the effectiveness of the Patch Management Program.



Vulnerability Mitigation
The following chart demonstrates the effectiveness of the mitigation strategy for the top vulnerable programs from Virginia Bankers Association's previous Vulnerability Assessment.