Enterprise Vulnerability & Patch Management

Agenda

❖ Overall windows server authentication scan status and summary.

❖ Overall vulnerability summary

❖ Prioritization based on Zero (Confirmed & Potential) & (Key Risk exploits)

❖ Overall Vulnerability Remediation Strategy (Stage 1 & Stage 2).

❖ Stage 1 Remediation plan based on vulnerability summary.

Key Highlights: Windows Server Authenticated Scan

Overall Windows – Baseline Status

Details	IP's Count
No. of Assets considered for baseline *	2652

** Post successful authentication*

No. of Assets Failed during Baselining **

No. of failed authentication	**49**
No. of assets authentication not attempted	24
No. of assets not live	393
Total	**466**

Vulnerability Categories/ Rating	Immediate	Critical	High	Medium	Low	Grand Total
MS Windows Patching	8055	23783	4677	831		37346
Software Update/ Uninstallation	5466	27358	14925	2966	1672	52387
EOL/ Obsolete	4083					4083
OS Hardening (configuration)	120	2735	37343	34132	356	74686
Grand Total	**17724**	**53876**	**56945**	**37929**	**2028**	**168502**

Legends

- Patching: MS – Patches & components (MS Office/ SQL, Oracle, JAVA JRE, Apache tomcat, etc.)
- S/W Update/ Uninstallation: Categorized for utility tools/ Apps like, WinZip, Zoom, 7Zip, Google Chrome, etc.
- EOL/ Obsolete: End of life and obsolete vulnerabilities on OS, applications, middleware, etc.
- Configuration: OS hardening/ configuration (GPO/ Registry entries, TLS/ SSL version/ cipher suite etc.)

Severity	CVSS Score	Timeline	Description
Immediate	Top priority	0 - 02 days	Intruders can easily gain control of the host, might compromise entire network security, including full read & write access, remote execution of commands, and the presence of backdoors
Critical	9.0-10.0	0 – 05 days	Intruders can possibly gain control of the host, might lead to potential leakage of highly sensitive information, including full read access, potential backdoors, or a listing of all the users on the host.
High	7.0-8.9	0 - 30 days	Intruders can gain access to specific information, including security settings. potential misuse of the host by intruders, including vulnerabilities at this level may include partial disclosure, access to certain files, directory browsing, disclosure of filtering rules and security mechanisms, DOS attacks, and unauthorized use of services.
Medium	4.0-6.9	0 - 60 days	Intruders can collect sensitive information, such as the precise version of software installed. Intruders can easily exploit known vulnerabilities specific to software versions
Low	0.1-3.9	0 - 90 days	Intruders can collect information about open ports, services, etc. and may be able to use this information to find other vulnerabilities.

*Disclaimer – * Remediation SLA will be factored after project go-live date (ETA – 15th Jan'24)*

Key Highlights: Windows Server Authenticated Scan

Zero-Day Vulnerability - Confirmed Threat

Vulnerability Title	CRITICAL	HIGH	MEDIUM	Grand Total
EOL/Obsolete Software: Apache HTTP Server 2.2.x Detected	124			124
Microsoft Exchange Server Multiple Vulnerabilities (ProxyNotShell) (Unauthenticated Check)		8		8
Microsoft SQL Server Database Link Crawling Command Execution - Zero Day			116	116
Version Control System Files Exposed by the Web Server			3	3
Windows Unquoted/Trusted Service Paths Privilege Escalation Security Issue			1146	1146
Grand Total	**124**	**8**	**1265**	**1397**

Zero-Day Vulnerability – Potential Threat

Vulnerability Title	CRITICAL	HIGH	MEDIUM	Grand Total
Microsoft Group Converter (grpconv.exe) Arbitrary DLL Preloading Vulnerability - Zero Day	3			3
Microsoft Windows "RunAs" Password Length Local Information Disclosure - Zero Day			14	14
Microsoft Windows Help File Heap Based Buffer Overflow - Zero Day			3	3
Microsoft Windows PNG File IHDR Block Denial of Service Vulnerability - Zero Day			6	6
Microsoft Word 2007 WWLib.DLL Unspecified Document File Buffer Overflow Vulnerability - Zero Day			3	3
Oracle VM VirtualBox E1000 Guest-to-Host Escape Vulnerability (Zero Day)	1			1
Webmin Package Updates Remote Command Execution Vulnerability		1		1
Windows Service Weak Permissions detected			135	135
Grand Total	**4**	**1**	**161**	**166**

Risk	Impact
Data loss, Ransomware, System compromise etc.	Data leakage (Sensitive info), Org Security score impact etc

Key Highlights: Windows Server Authenticated Scan

Key Exploits based on Software Update/Uninstallation

Software	Critical	High	Immediate	Medium	Grand Total
7-Zip	1200				1200
Adobe Acrobat Reader	185	2	9		196
Adobe Flash player	227		427		654
Google Chrome	510	99	58	4	671
Internet Explorer	911	607	1151		2669
Microsoft Office	798	8	149		955
Microsoft SharePoint	119	28	6		153
Mozilla Firefox	712	281	217		1210
TeamViewer	1	1			2
WinRAR	12	4			16
WinSCP	2	19			21
Wireshark	99	387		6	492
Zoom	21	35		11	67
Grand Total	**4797**	**1471**	**2017**	**21**	**8306**

Key Exploits based on OS Hardening/Configuration

Vulnerability	Critical	Medium	Grand Total
Account Brute Force Possible Through IIS NTLM Authentication Scheme		13	13
Detected LanMan/NTLMv1 Authentication method	82		82
Microsoft Windows Explorer AutoPlay Not Disabled		174	174
Microsoft Windows Telnet Server Does Not Enforce NTLM Authentication		2	2
Remote User List Disclosure Using NetBIOS	4		4
Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Factoring RSA_EXPORT Keys Vulnerability (FREAK)	7		7
Webmin Package Updates Remote Command Execution Vulnerability	1		1

Key Highlights: Windows Server Authenticated Scan

Key Exploits based on Windows Patching

Operating System	Critical	High	Immediate	Grand Total
Windows (R) Storage Server 2008 Standard Service Pack 2	41	3	16	60
Windows 2003 R2 Service Pack 2			9	9
Windows 2008 Enterprise Server 64 bit Edition Service Pack 2	194	17	78	289
Windows 2008 Enterprise Server Service Pack 2	253	27	123	403
Windows 2008 R2 Enterprise Service Pack 1			13	13
Windows 2008 R2 Standard Service Pack 1			15	15
Windows 2012 R2 Standard			1	1
Windows 2016		1	4	5
Windows Server 2003 R2 Service Pack 2	18	26	21	65
Windows Server 2008 R2 Enterprise 64 bit Edition Service Pack 1	2615	97	1158	3870
Windows Server 2008 R2 Standard 64 bit Edition Service Pack 1	5200	121	2152	7473
Windows Server 2012 R2 Core 64 bit Edition	1			1
Windows Server 2012 R2 Datacenter 64 bit Edition	68	8	22	98
Windows Server 2012 R2 Standard 64 bit Edition	4974	350	1931	7255
Windows Server 2012 Standard 64 bit Edition	9	4	2	15
Windows Server 2016 Datacenter 64 bit Edition Version 1607	212	12	51	275
Windows Server 2016 Standard 64 bit Edition Version 1607	3242	92	953	4287
Windows Server 2016 Standard Version 1607			2	2
Windows Server 2019 Datacenter 64 bit Edition Version 1809 Build 17763	297	16	102	415
Windows Server 2019 Standard 64 bit Edition Version 1809 Build 17763	2734	475	1157	4366
Windows Server 2022 Datacenter Version 21H2	6		5	11
Windows Vista / Windows 2008			1	1
Grand Total	**19864**	**1249**	**7816**	**28929**

Summary of Vulnerability Remediation Strategy

Stage - 1: Remediation Plan

#	Description	Total	Remediation Target	Balance	Timeline
1	Windows Patching	37346	37346	0	TBD
2	Software update/ Uninstallation	52387	17724	34663	TBD
3	EOL/ Obsolete	4083	1314	2769	TBD
4	OS Hardening/ Configuration	74686	1555	73131	TBD
	Total	**168502**	**57939**	**110563**	

***Remediation Target includes Exploits*

Stage - 2: Remediation Plan (DRAFT)

#	Description	Total	Remediation Target	Balance	Timeline
1	Windows Patching	0	NA	0	NA
2	Software update/ Uninstallation	34663	TBD	0	TBD
3	EOL/ Obsolete	2769	TBD	0	TBD
4	OS Hardening/ Configuration	73131	TBD	0	TBD
	Total	**110563**	**TBD**	**0**	

Stage – 1 Windows Patching Explained

Operating System	Immediate	Critical	High	Medium	Grand Total
Windows 2003 R2 Service Pack 2	9			6	15
Windows 2008 Enterprise Server 64 bit Edition Service Pack 2	79	235	80	25	419
Windows 2008 Enterprise Server Service Pack 2	147	353	120	28	648
Windows 2008 R2 Enterprise Service Pack 1	13				13
Windows 2008 R2 Standard Service Pack 1	15				15
Windows 2012 R2 Standard	1				1
Windows 2016	4		1		5
Windows Server 2003 R2 Service Pack 2	21	40	32	9	102
Windows Server 2008 R2 Enterprise 64 bit Edition Service Pack 1	1194	3080	746	166	5186
Windows Server 2008 R2 Standard 64 bit Edition Service Pack 1	2229	6142	1453	492	10316
Windows Server 2012 R2 Core 64 bit Edition		1			1
Windows Server 2012 R2 Datacenter 64 bit Edition	22	82	16		120
Windows Server 2012 R2 Standard 64 bit Edition	2011	6030	973	34	9048
Windows Server 2012 Standard 64 bit Edition	2	12	10		24
Windows Server 2016 Datacenter 64 bit Edition Version 1607	52	276	28		356
Windows Server 2016 Standard 64 bit Edition Version 1607	965	4249	389	15	5618
Windows Server 2016 Standard Version 1607			2		2
Windows Server 2019 Datacenter 64 bit Edition Version 1809 Build 17763	105	326	66	2	499
Windows Server 2019 Standard 64 bit Edition Version 1809 Build 17763	1164	2903	746	51	4864
Windows Server 2022 Datacenter Version 21H2	5	7			12
Windows Vista / Windows 2008	1				1
Grand Total	**8039**	**23736**	**4662**	**828**	**37265**

Stage – 1 Software Update/ Uninstallation: Explained

Software	Critical	High	Immediate	Medium	Grand Total
7-Zip	1200	615			1815
Adobe Acrobat Reader	222	14	44	3	283
Adobe Flash player	554	33	590		1177
Google Chrome	724	137	58	8	927
Internet Explorer	3806	826	1332	61	6025
MS Office	2164	70	337		2571
MS SharePoint	474	76	21		571
Mozilla Firefox	2072	483	304		2859
TeamViewer	2	2	1		5
WinRAR	12	11		7	30
WinSCP	25	75			100
Wireshark	287	593		8	888
Zoom	203	175	24	71	473
Grand Total	**11745**	**3110**	**2711**	**158**	**17724**

Stage – 1 EOL/ Obsolete: Explained

EOL	Immediate
Adobe Flash 10.x Detected	2
Adobe Flash Player Detected	46
Adobe Reader 10.x Detected	2
Adobe Reader 9.x Detected	21
Adobe Reader/Acrobat XI Detected	55
MS Internet Explorer 10 Detected	6
MS Internet Explorer 11 Detected	133
MS Internet Explorer 7 Detected	1
MS Internet Explorer 8 Detected	19
MS Internet Explorer 9 Detected	4
MS Office 2000 & 2003 Web Components	3
MS Office 2003 Detected	1
MS Office 2003 RTM Detected	1
MS Office 2007 Detected	3
MS Office 2010 RTM Detected	2
Part 1 Total	**299**

EOL	Immediate
MS Office 2010 Service Pack 1 (SP1) Detected	29
MS Office 2010 Service Pack 2 (SP2) Detected	20
MS PowerPoint Viewer Detected	2
MS Silverlight 5 Detected	931
MS Word Viewer Detected	1
Mozilla Firefox Prior to 81 Detected	7
Unsupported WinZip Installation 20.5 and Prior Detected	1
Wireshark 1.10 Detected	3
Wireshark 1.12 Detected	1
Wireshark 1.4 Detected	1
Wireshark 1.8.x Detected	2
Wireshark 2.0 Detected	1
Wireshark 2.2 Detected	2
Wireshark 2.4 Detected	2
Wireshark 2.6 Detected	7
Wireshark 3.0 Detected	5
Part 2 Total	**1015**

EOL	Immediate
Part 1 Total	299
Part 2 Total	1015
Grand Total	**1314**

Stage - 1 OS Hardening/ Configuration: Explained

OS Hardening/Configuration	Critical	Medium	Grand Total
Account Brute Force Possible Through IIS NTLM Authentication Scheme		13	13
Detected LanMan/NTLMv1 Authentication method	82		82
Microsoft Windows Explorer AutoPlay Not Disabled		174	174
Microsoft Windows Telnet Server Does Not Enforce NTLM Authentication		2	2
Windows Explorer Autoplay Not Disabled for Default User		197	197
Null Session/Password NetBIOS Access	4		4
Potential TCP Backdoor	47		47
Potential UDP Backdoor	21		21
Remote User List Disclosure Using NetBIOS	4		4
Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Factoring RSA_EXPORT Keys Vulnerability (FREAK)	7		7
SSL Server Allows Anonymous Authentication Vulnerability	9		9
SSL Server Allows Cleartext Communication Vulnerability	4		4
Unauthenticated Dynamic DNS Updates Allow DNS Poisoning Vulnerability	2		2
Weak SSL/TLS Key Exchange	987		987
Webmin Package Updates Remote Command Execution Vulnerability	1		1
Webmin XXE Vulnerability authenticated Remote Code Execution	1		1
Grand Total	**1169**	**386**	**1555**