DYOPATH

SECURITY ASSESSMENT REPORT

PREPARED FOR:
Your Company Name

CONTACT:
FirstName LastName
Your Title

1.866.609.PATH

solutions@dyopath.com

PREPARED BY:
DYOPATH Security Practice Lead

REVISED:
XX/XX/XXXX

TABLE OF

CONTENTS

1. EXECUTIVE SUMMARY

1.1 Background

COMPANY NAME sought to improve its overall security posture and therefore engaged DYOPATH to perform a security assessment and document the results in this report. This assessment's primary driver was to provide a "second set of eyes" for **COMPANY NAME** to better meet the challenges of the modern threat landscape.

1.2 Results

COMPANY NAME's environment has several positive elements; however, improvement is needed, most notably with vulnerabilities from outdated software, documentation, and policy settings. A summary view of the detailed findings is presented immediately below, along with the more important and general themes noted throughout the detailed findings under the Summary Findings in the next section below.

	Number of Detailed Findings		
Scope Area	Critical	High	Medium
Penetration Testing	1	1	3
Configuration and Architecture	1	1	3
Controls	3	0	1

1.3 Scope

DYOPATH performed the fieldwork beginning **08/20/23** and concluding the week of **09/21/23**.

Specifically, DYOPATH performed the following services:

- Assessed the controls, configuration and architecture, including:
  - an assessment against the **[CIS Top 20 Framework]** that evaluates **COMPANY NAME's** overall security posture adherence to the CIS guidelines
  - a detailed analysis of **COMPANY NAME's** Infrastructure, including the network, servers, Active Directory, cloud, and email configurations

- Performed Vulnerability scans and Penetration Testing against **COMPANY NAME's** external and internal IT resources:
  - the external penetration test and vulnerability assessment focused on **COMPANY NAME's** IT resources accessible from the public Internet including:

    [list IP addresses or cross reference to an Appendix]

  - the internal penetration test and vulnerability assessment focused on **COMPANY NAME's** IT resources accessible by an actor with some level of access to a network behind the perimeter firewall including:

    [list IP addresses or cross reference to an Appendix]

- Documented areas of specific concern where potential threats to the security and integrity of processes and information are present; and

- Developed this analysis report detailing the areas of concern and recommendations for mitigation of identified risks and vulnerabilities.

2. OBSERVATIONS AND RECOMMENDATIONS

2.1 Summary Findings

The key findings are in the table below. These findings are a moment-in-time snapshot, and therefore, additional diligence will be necessary to keep pace with changes in threats, vulnerabilities, and control expectations. The findings are based on automated vulnerability scanning tools, manual penetration testing techniques, interviews, and inspection of configuration settings (either manually or through proprietary scripts). The table includes a Discovery Source that indicates which task of the project resulted in the finding, an estimated risk and level of remediation effort, and summary recommendations along with "quick wins" where possible.

The following section includes additional comments on detailed vulnerabilities and configuration improvements. DYOPATH gave detailed technical results to **COMPANY NAME** IT personnel, as appropriate. In addition, a quick overview slide has been provided in Appendix A to provide a more visual presentation of the findings in this report.

Table 2 - High-Level Findings

Finding Area / Title	Discovery Source	Risk	Recommendations (suggested timing)
Out-of-Date Software / Vulnerability Management Improvements The tester noted a couple of significant vulnerabilities on the internal network. These vulnerabilities could allow unauthorized access to systems or data.	Configuration & Architecture Assessment	High	Review the prioritized list of vulnerabilities on the vulnerability table below and apply appropriate updates. (30 days or less) Adopt a process to scan for and remediate vulnerabilities periodically. (3 to 6 months) Isolate legacy applications or systems where it is not possible to quickly patch or remediate vulnerabilities. (3 to 6 months)
EDR Effectiveness The security tester was able to gain complete control over the entire IT environment after demonstrating several software-based security holes. This indicates that the deployed Endpoint Detection and Response (EDR) solution was ineffective. Please note that the security tester was provided Local Admin privileges; however, jumping from an end user's privileges to local admin is not entirely preventable with just native operating system controls.	Vulnerability Scanning	High	Apply Password protection to the uninstallation of the existing EDR as an interim solution. (30 days or less) Update or upgrade the current EDR solution If possible. (1 year)
Security Monitoring The security tester was able to gain complete control over the entire IT environment undetected, which may indicate ineffective security monitoring.	Configuration & Architecture Assessment	High	Develop an operational process to regularly spot-check logs for a range of activities, including new accounts, strange login locations, and interesting command line usage. (30 days) Consider deployment of a system to consolidate logs and provide automated alerting capabilities. (1 year)
Control Documentation & Practices Noted numerous opportunities for improvement if following the CIS Top 20 guidelines.	Control Assessment	Moderate	Review the control assessment later in this document and establish an action plan starting with forming a security program and appropriate governance groups. (1 year)
Windows Security Hardening Improvements Some Windows security settings need improvement, most notably Active Directory policy settings for password and network security.	Configuration & Architecture Assessment	Moderate	Review the list of prioritized security settings in this report and plan to update the settings where feasible. (3 months for the top ten provided in this report) A complete list with hundreds of settings is also provided separately from this report to configure enhanced hardening for Windows servers and devices. (6 months)

3. DETAILED RESULTS AND RECOMMENDATIONS

The following sections provide supporting details for each significant area's findings included in this project's scope.

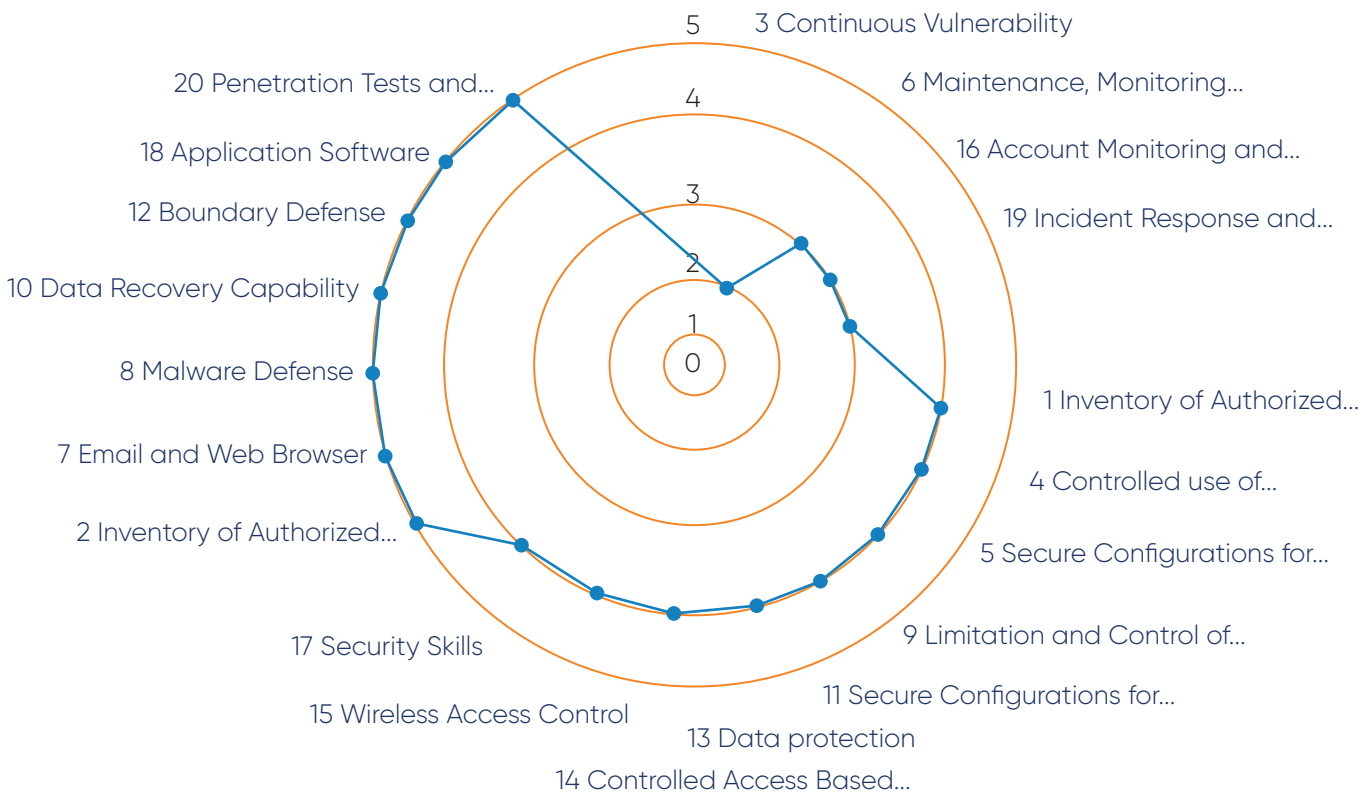
3.1 Controls Assessment

A gap assessment of **COMPANY NAME's** cybersecurity controls against the CIS Top 20 was performed. The CIS Top 20 is a set of control objectives widely held as a gold standard for security controls. The results and recommendations are reflected in the table below. They indicate initial coverage for many controls, some good coverage areas, and some possible places for improvement.

The average score determined by the observed controls was 4.

Control Score	Control Status	Control Score Criteria
0	Non-Existent	There is no evidence of the organization meeting the objective.
1	Initial	The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
2	Repeatable	The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
3	Defined	The organization has a documented, detailed approach to meeting the objective and regularly measures its compliance.
4	Managed	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond applicable regulations requirements.
5	Optimized	The organization has refined its standards and practices, focusing on improving its capabilities most efficiently and cost-effectively.

Control Coverage Map



The detail supporting the above summary chart is provided in the below table.

Ref	Test Area	Results	Rating	Risk	Recommendations
1	Inventory of Authorized and Unauthorized Devices	Devices are deployed with LogMeIn remote management tools. Software and hardware inventory can be pulled and reviewed as needed.	4	Unauthorized devices could potentially access company resources by plugging into a hub or spoke office network ports/live jacks.	Deploy a network access control system could identify any unauthorized devices that have attempted to connect to the internal network and ensure they can't reach them.
2	Inventory of Authorized and Unauthorized Software	Software inventory can be pulled through LogMeIn management tools. This is reviewed on an as-needed basis. Most users are not admins and cannot install software on their devices by themselves.	5	Little to no risk of exploits	No recommendations.
3	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
4	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

ADDITIONAL INFORMATION AVAILABLE UPON COMPLETION OF ASSESSMENT

3.2 Desktop Security Assessment Results

The below analysis includes an assessment of a standard desktop provided by **COMPANY NAME.**

Ref	Test Area	Results	Recommendations
1	Determine if SMB signing is enforced and blocking relays.	Fail – Successfully relayed a hash gathered from the test device.	Ensure SMBv3 is enforced and enable SMB signing if possible
2	Determine whether a firewall is enabled.	Pass – firewall enabled	-
3	Determine whether security updates are deployed for the operating system.	Fail – updates enabled but behind on a few critical systems, including an ESX host. ESX hosts and was able to successfully run test read commands against hosts.	-
4	Inventory the software installs and determine whether there is out-of-date or unpatched 3rd party software.	Pass – none found	Vulnerability scans would be useful in finding these as they occur, especially in desktop devices.

ADDITIONAL INFORMATION AVAILABLE UPON COMPLETION OF ASSESSMENT

Internal Vulnerabilities Table

Vulnerability Name	Risk Description	Recommendations
VCenter virtual SAN health check plugin RCE (CVE-2021-21985) Observed on host: 10.x.x.x	The VSphere client (HTML 5) does not sanitize inputs well and allows remote code execution on the host before as well as VMWare cloud foundations 4.x before 4.21	Apply patches described here to the affected

ADDITIONAL INFORMATION AVAILABLE UPON COMPLETION OF ASSESSMENT

3.3 Network/Firewall, Email & Spam

An analysis of the firewall and email settings was performed, which follows. DYOPATH noted reasonably secure settings in this area, with some areas for improvement.

Ref	Procedure	Results	Recommendations
1	Inspect firewall configuration and architecture for design weaknesses, undocumented firewall rules, or port issues	Pass - there is a Meraki firewall configured with VPNs that are relatively secure. IPS and threat detections sourcing from AMP libraries is enabled on the devices.	-
2	Note which interfaces are present and which networks they connect to gain an understanding of trusted and untrusted zones and traffic	Pass - DMZ only hosts DUO two-factor proxy	-
3	Note direct TCP, UDP, or ICMP port access from WAN to LAN, noted from WAN to a proper DMZ	Pass - Public NAT is in place for a hybrid Exchange server. However, firewall rules limit all other traffic to devices on the VPN or in a spoke office network.	Consider tightening allowed traffic from spoke offices to the hub network. Restrictions based on allowed applications or needed ports.

ADDITIONAL INFORMATION AVAILABLE UPON COMPLETION OF ASSESSMENT

3.4 Office 365/Azure

An analysis of the Office 365/Azure was performed, which follows. DYOPATH noted reasonably secure settings in this area, with some areas for improvement.

Step	Procedure	Results	Recommendations
1	Admin logs are enabled and tracking correctly	Logs are enabled and showing correctly.	-
2	Alerting on high-impact changes is configured and alerting appropriate people.	Alerts for high-impact issues are configured and notifying the IT group appropriately.	-
3	Legacy protocols have been disabled or restricted to only devices that need them.	Legacy protocols have been disabled and do not allow access without going through MFA.	-

ADDITIONAL INFORMATION AVAILABLE UPON COMPLETION OF ASSESSMENT

3.5 Active Directory

DYOPATH analyzed Active Directory for weaknesses and determined the environment was reasonably well configured, with some improvement opportunities. Several configuration recommendations follow based on the Center for Internet Security's level 1 baseline.

Ref #	Test Area	Results	Recommendations
1	Compare the CIS Level 1 Baseline AD Group Policy Object (GPO) settings against the AD environment settings.	Completed	See the CIS baseline table below.
2	Alerting on high-impact changes is configured and alerting appropriate people.	Alerts for high-impact issues are configured and notifying the IT group appropriately.	See below
3	Legacy protocols have been disabled or restricted to only devices that need them.	Legacy protocols have been disabled and do not allow access without going through MFA.	-

ADDITIONAL INFORMATION AVAILABLE UPON COMPLETION OF ASSESSMENT

CIS Baseline Level Table

Ref #	Policy Area	Policy Settings (Windows Registry) Reference	CIS Baseline Level 1 Recommended Value	Result
1	User Policy	Minimum password age	1 or more day(s)	Pass
2	[illegible]	[illegible]	[illegible]	[illegible]
3	[illegible]	[illegible]	[illegible]	[illegible]
4	[illegible]	[illegible]	[illegible]	[illegible]

ADDITIONAL INFORMATION AVAILABLE UPON COMPLETION OF ASSESSMENT

4. SOCIAL ENGINEERING PENETRATION TEST RESULTS

The following procedures describe the results of an internal penetration test performed on the inside (behind the firewall) of the **COMPANY NAME** environment. Rules of engagement for physical penetration testing are detailed in Appendix A of this document. DYOPATH staff adhered to all rules of engagement during attempts made to social engineer **COMPANY NAME** employees and enter restricted areas of the Houston office on **STREET NAME.** Access was attempted by convincing individual employees to grant DYOPATH access into a secure area. In addition, DYOPATH personnel checked in with Houston Police Officers at the front desk prior to attempting any reconnaissance or penetration tests.

DYOPATH used the following scale to grade each attempt based on the results:

GRADE 3 = Attempt is blocked at door or within ten (10) feet of door once inside.

GRADE 2 = Door is breached beyond ten (10) feet inside, but attempt is identified and blocked before Operative can collect information.

GRADE 1 = Door is fully breached and was able to take possession of a workstation. Operative attempted to collect information but workstation was locked.

GRADE 0 = Total failure – Operative was able to fully breach, compromise a workstation, and collect private consumer information.

The following table summarizes the social engineering attempts documented in the paragraph below:

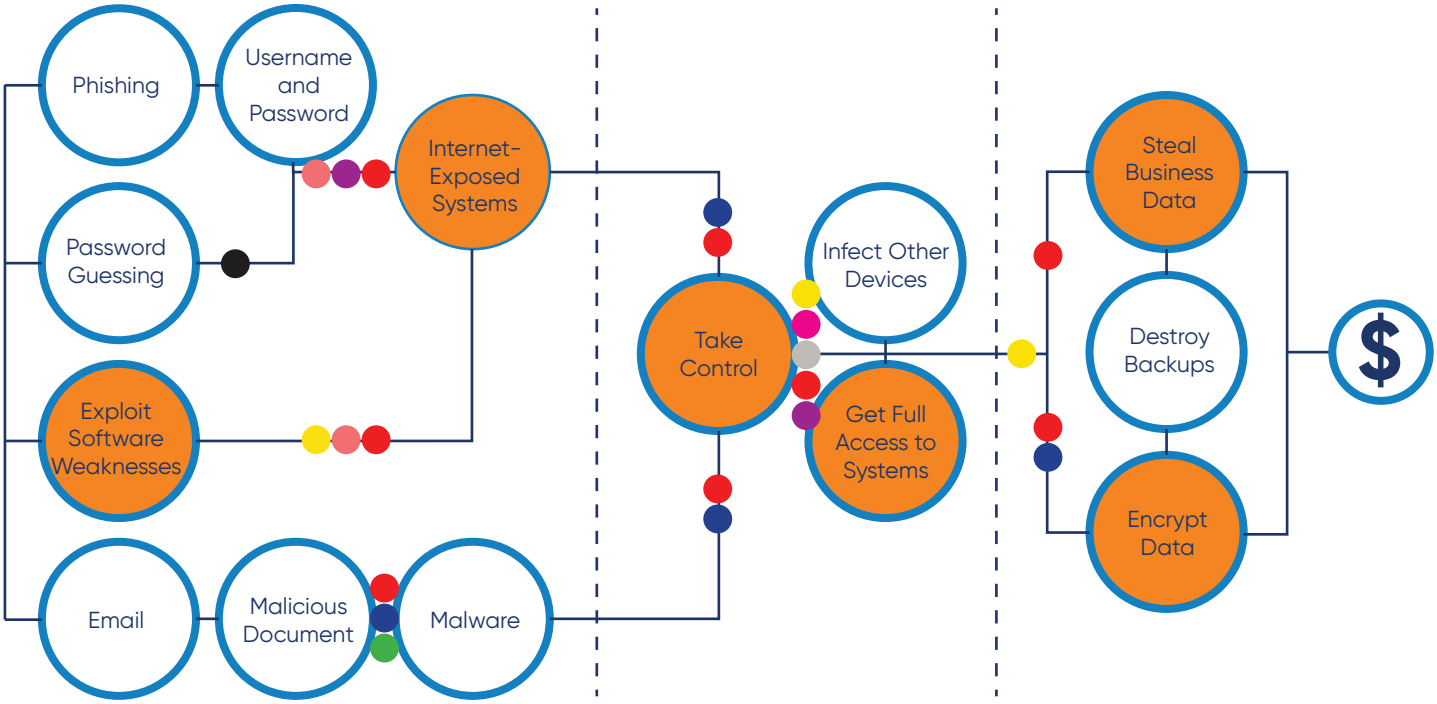
KEY:

GRADE 0	GRADE 1	GRADE 2	GRADE 3

Door #	Attempts	Successes	Minutes Inside	Grade	Notes
1	2	1	2	3	1st attempt Door was propped open by door stopper. 2nd breach attempt failed at door;
1	2	1	2	2	1st attempt Door was propped open by door stopper. 2nd breach attempt failed at door;
1	**ADDITIONAL INFORMATION AVAILABLE UPON COMPLETION OF ASSESSMENT**				1st attempt Door was propped open by door stopper. 2nd breach attempt failed at door;
1	2	1	2	3	1st attempt Door was propped open by door stopper. 2nd breach attempt failed at door;
1	2	1	2	0	1st attempt Door was propped open by door stopper. 2nd breach attempt failed at door;

APPENDIX A. KEY TECHNICAL CONTROLS

The below diagram portrays the areas where key technical controls are typically needed to prevent risks from threats such as ransomware. During this engagement, some areas were found to have weaknesses that could be sufficient to gain control over the entire IT environment or deliver an effective ransomware attack. These more vulnerable areas are covered with an orange transparent circle.



Technical Control Key
Firewall
Backups
Patching
Application White-Listing
Multi-Factor Authentication
SIEM / SOC
Network Segmentation
Disable Macros
Least Privilege
Password Vault

APPENDIX B. FIGURES

The figures below are screenshot examples of the testing procedures and other evidence referenced from the preceding tables.

Figure 1: Response from SAN plugin from Vulnerable vSphere client

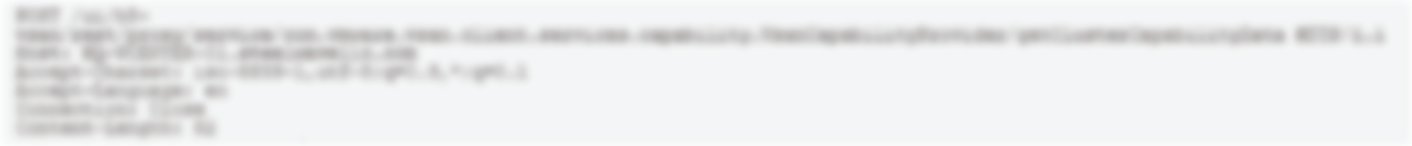
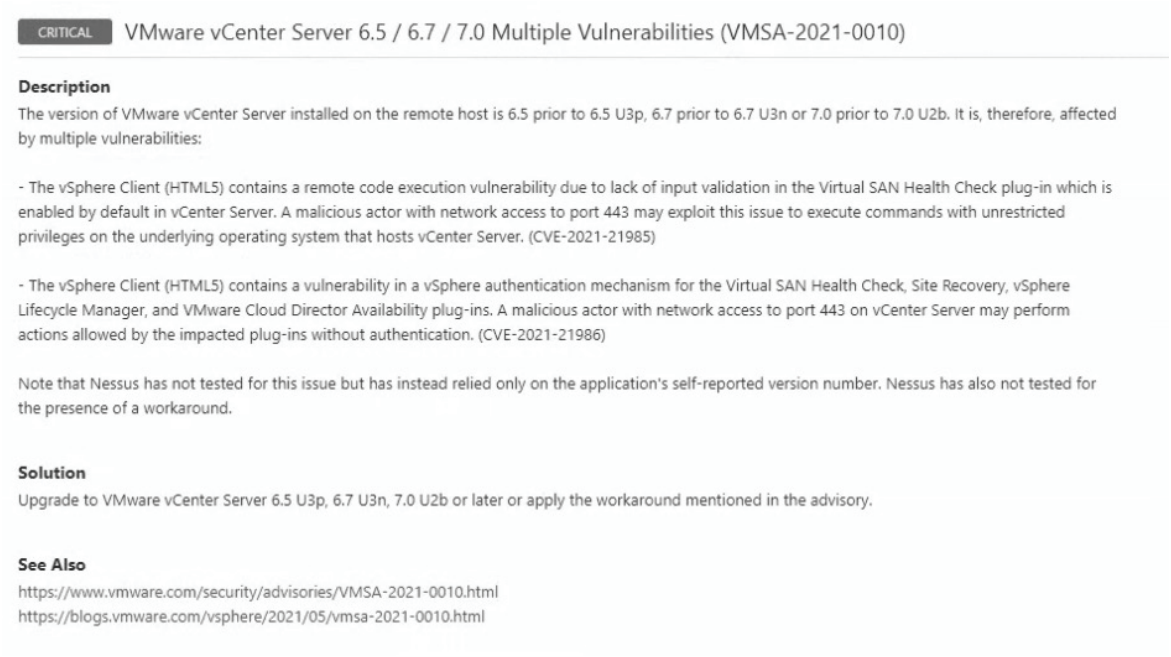


Figure 2: The detailed output from the advanced scanner run against the vulnerable vSphere client.



CRITICAL VMware vCenter Server 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0010)

Description

The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5 U3p, 6.7 prior to 6.7 U3n or 7.0 prior to 7.0 U2b. It is, therefore, affected by multiple vulnerabilities:

- The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. (CVE-2021-21985)

- The vSphere Client (HTML5) contains a vulnerability in a vSphere authentication mechanism for the Virtual SAN Health Check, Site Recovery, vSphere Lifecycle Manager, and VMware Cloud Director Availability plug-ins. A malicious actor with network access to port 443 on vCenter Server may perform actions allowed by the impacted plug-ins without authentication. (CVE-2021-21986)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. Nessus has also not tested for the presence of a workaround.

Solution

Upgrade to VMware vCenter Server 6.5 U3p, 6.7 U3n, 7.0 U2b or later or apply the workaround mentioned in the advisory.

See Also

https://www.vmware.com/security/advisories/VMSA-2021-0010.html
https://blogs.vmware.com/vsphere/2021/05/vmsa-2021-0010.html

Figure 3: Firewall rules from Meraki hub network.

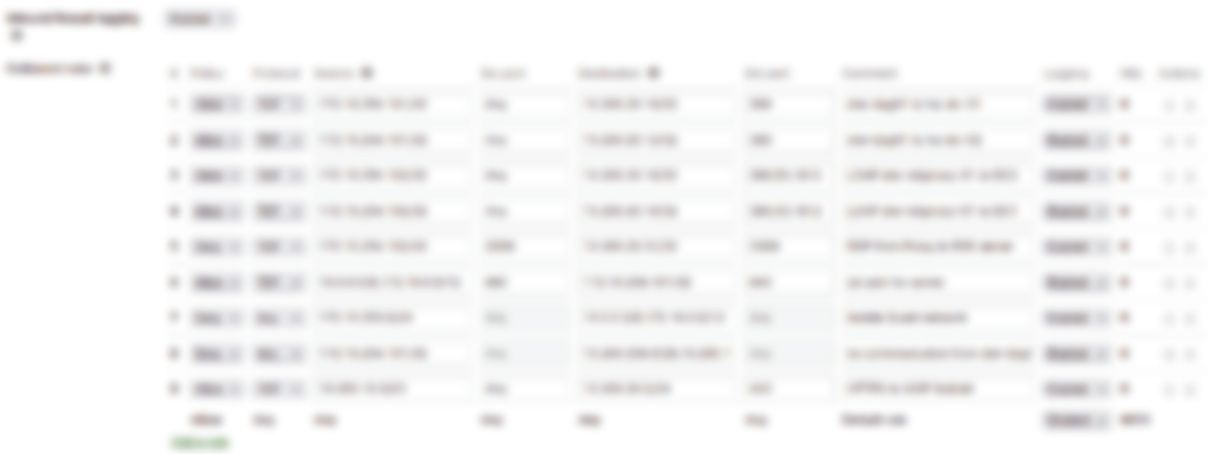


Figure 4: No restrictions on outbound traffic from hub network firewall.

Site-to-site outbound firewall

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Logging
	Allow	Any	Any	Any	Any	Any	Default rule	Enabled

Figure 5: SNMP setting on the Meraki Devices.

Figure 6: AD Group membership exported from escalated access to domain controllers. (Evidence of LDAP accounts with full domain admin access.)

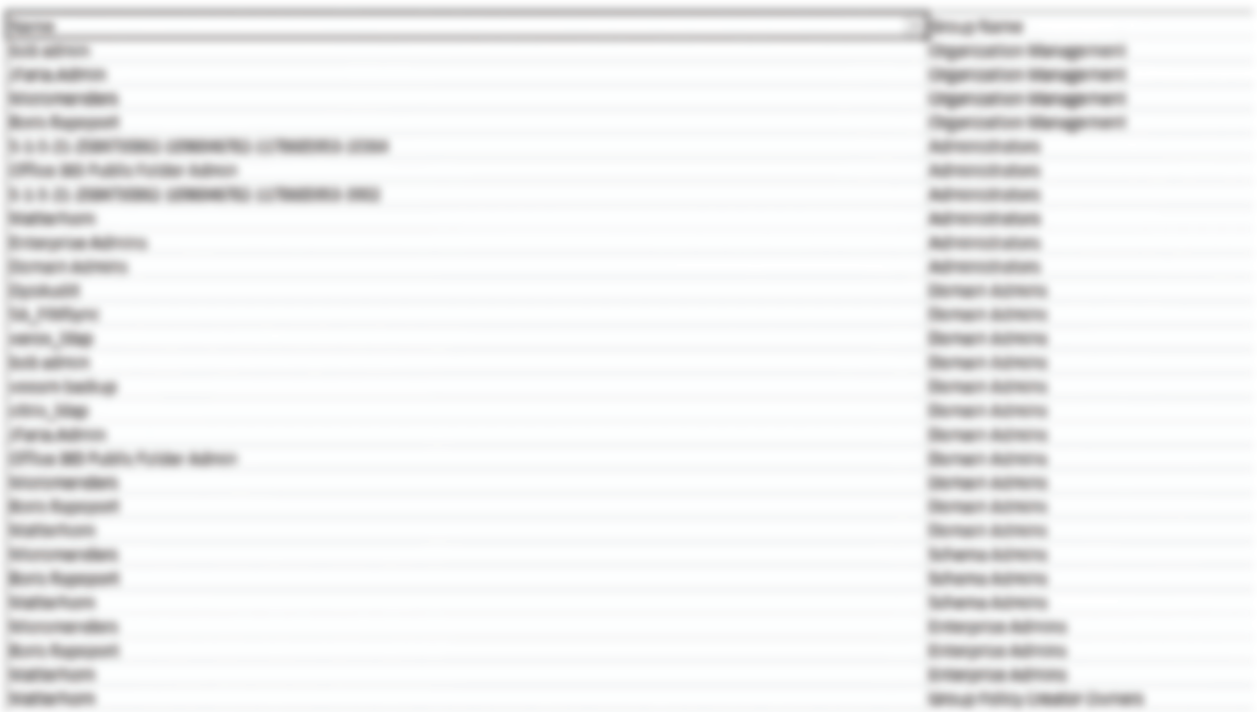


Figure 7: Evidence of SMB access to the domain controller in the network.

Figure 8: Command used to install PowerShell remote access tools on the test device.

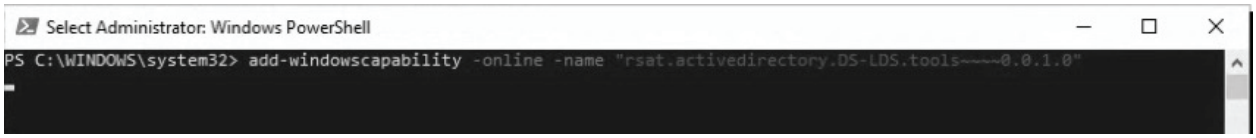


Figure 9: Evidence of new account creation on newly elevated access on the domain controller.

Figure 10: Test account created on file share server after successful SMB relay attack.

END OF ASSESSMENT REPORT

DYOPATH