Subject: QTR1 Vulnerability Scan Summary [Internal Systems] **Date**: February 4th, 2025
Tools Used: Nessus Essentials version 10.6.0 **Prepared By:** Jordan C. Lanning
Scan Date: February 1st, 2025

TARGETS SCANNED

1. WIN-10-USER01 (192.168.1.10)
2. UBUNTU-SERVER01 (192.168.1.15)
3. Router Admin Interface (192.168.1.1)

EXECUTIVE SUMMARY

This vulnerability assessment was performed in accordance with company policies and procedures. The scan revealed several medium and high-severity vulnerabilities primarily related to missing patches, outdated services, and insecure configurations. There were a total of 22 total vulnerabilities.

- 18 vulnerabilities are already documented within the risk register and have compensating controls on systems that cannot be patched.
- 4 new high-priority vulnerabilities require immediate attention and are outlined below.

FINDINGS SUMMARY

Severity	Count
Critical	0
High	4
Medium	8
Low	10

TOP FINDINGS

1. CVE-2017-0143 – Windows SMBv1 Remote Code Execution Vulnerability
    a. **Severity**: HIGH (CVSS v3.0: 8.8)
    b. **Description**: The SMBv1 server allows the remote attackers to execute arbitrary code via crafted packets.
    c. **Recommendation**: Per Microsoft's guidance, there are no fixes. However, there are compensating controls that are available. For this organization, it is recommended to disable SMBv1 on customers using Windows Vista or Later.
2. CVE-2021-41617 – OpenSSH Privilege Escalation Vulnerability
    a. **Severity**: HIGH (CVSS v3.1: 7.0)
    b. **Description**: This vulnerability allows for privilege escalation because supplemental groups are not initialized as expected. Group memberships of the sshd process are typically used here.
    c. **Recommendation**: Per Red Hat Linux's Product Security, there is not an available mitigation available. OpenSSH developers recommends for similar vulnerabilities to enable PAM and disable AuthorizationKeysCommand where appropriate to reduce risk from similar privilege escalation scenarios.
3. CVE-2024-45697 – D-Link Routers Hidden Telnet Service Vulnerabity
    a. **Severity**: HIGH (CVSS v3.1: 8.8)
    b. **Description**: Certain models of D-Link wireless routers have a hidden functionality where the telnet service is enabled when the WAN port is plugged in. Unauthorized remote attackers can log in and execute OS commands using hard-coded credentials.

   c. **Recommendations**: Disable Telnet Service for the system.
4. CVE-2023-23397 – Microsoft Outlook Privilege Escalation via NTLM Leak
   a. **Severity**: MEDIUM (CVSS v3.1: 9.8)
   b. **Description**: Microsoft Outlook Privilege Escalation
   c. **Recommendation**: Block TCP 445/SMB outbound within firewall.

POA&M

TASK	PRIORITY	OWNER	DUE DATE
Disable SMBv1 on Windows Vista	HIGH	IT Admin	February 6th
Enable PAM, disable Auth-Key-CMD	HIGH	Linux Admin	February 8th
Disable Telnet	HIGH	Network Admin	February 8th
Update firewall to block TCP 445	HIGH	Network Admin	February 7th
Confirm compensating controls of previously known vulnerabilities	MEDIUM	System Owners	April 1st

CONCLUSION

The vulnerabilities identified in this assessment are manageable, with appropriate mitigations either already in place or easily implementable. If all remediations are completed as recommended, risk exposure will be significantly reduced or eliminated. A follow-up scan should be considered before QTR2 to confirm solution of outstanding issues. System owners are expected to maintain existing controls and take corrective action if any deviations are identified. We are updating our risk register to know the new exceptions.

There is **no substantial threat** to organizational systems at this time.

If there are any additional questions or concerns, please refer them Jordan C. Lanning, at 803-554-7322 or jordan.c.lanning@gmail.com. I will assist where I can.

Jordan C. Lanning, MPA, CySA+
Cybersecurity Analyst
803-554-7322