# Lab 4.1.1b Vulnerability Scanning

Thursday, July 20, 2023 4:37 PM

7.

A. 1 Critical rating
CVE-2023-21554, QueueJumper
Name: Microsoft Message Queuing RCE
ID: 175373
OS: Windows 10 (Lab 4.1.1b VM)

B. Microsoft Message Queuing Remote Code Execution Vulnerability
A message queuing application is affected by a remote code execution vulnerability.
CVSS rating: 9.8
**Solution:**
Apply updates in accordance with the vendor advisory.

Also See:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21554

C.

| Item: | IP Address | Rating | Impact |
|---|---|---|---|
| Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper) | 192.168.194.137 | 9.8 | Critical Impact. The Microsoft Message Queuing running on the remote host is affected by a remote code execution vulnerability. |
| CVE-1999-0103 Echo Service Detection CVE-1999-0635 | 192.168.194.137 | 5.0 | Medium Impact. Echo and chargen, or other combinations of UDP services, can be used in tandem to flood the server, a.k.a. UDP bomb or UDP packet storm. |
| CVE-1999-0103 Quote of the Day (QOTD) Service Detection | 192.168.194.137 | 5.0 | Medium Impact. An easy attack is 'pingpong' which IP spoofs a packet between two machines running Quote of the Day. This will cause them to spew characters at each other, slowing the machines down and saturating the network. |
| SMB Signing not required | 192.168.194.137 | 5.3 | Medium Impact. Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. |

D. Upon my vulnerability scan of Lab 4.1.1b VM, I discovered one "Critical" and three "Medium" impact vulnerabilities ranging in the above mentioned table. The system is at risk of remote code execution through Microsoft message queuing as well as execution of echo commands that jeopardize the software "Quote of the Day" (qotd). This requires immediate action.

E. Microsoft Message Queuing running on the remote host affected by the remote code execution vulnerability, has been deemed low complexity. This makes it easy for an attacker to send a specially crafted MSMQ file and execute a remote connection. In addition the Quote of the Day service makes the system vulnerable to a "pingpong" attack. This can slow the network or render it inoperable.