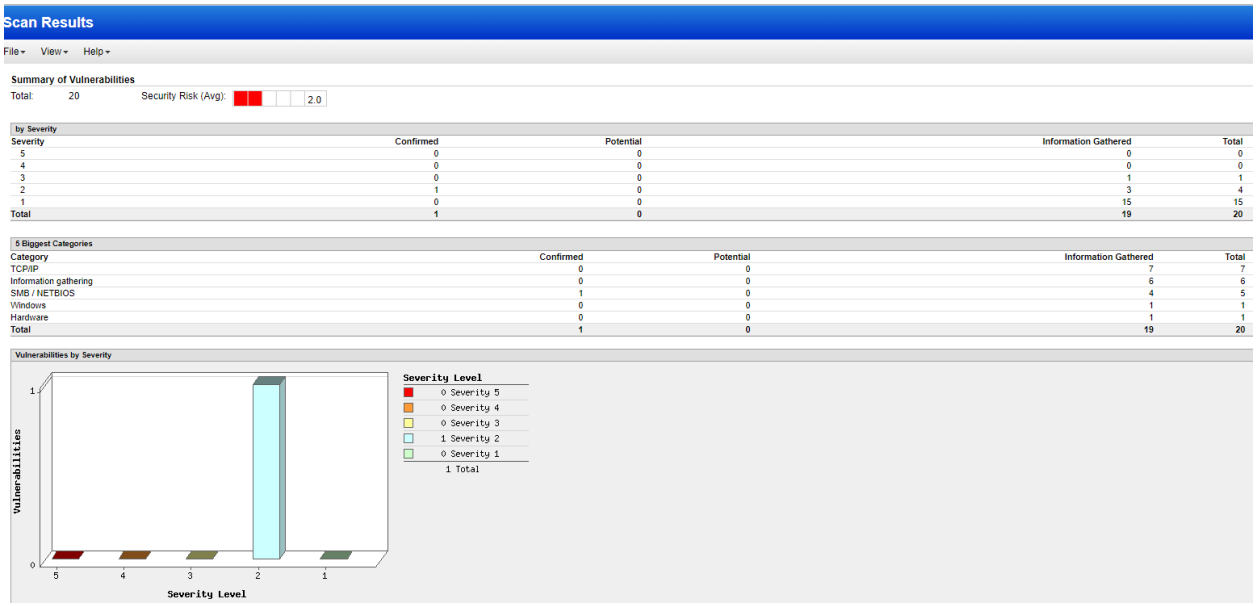
Vulnerability Management

Qualys Virtual Scanner

- Installed and Launched Qualys virtual scanner appliance on windows VM host and access software through Qualys Cloud Platform
- Implemented Vulnerability Management on sandbox networks:

  Discover, Prioritize, Asses, Report, Remediate,Verify

- Ran a non authenticated Scan on this network which showed 29 vulnerabilities



- Performed an Authenticated scan and discovered 117 vulnerabilities this authenticated scan gave me a more involved scan to help identify more potential harm that can corrupt my network or the potential company.

Excluded IPs: -

Option Profile: Basic Net Scan

Summary of Vulnerabilities

Total: 502 Security Risk (Avg): 5.0

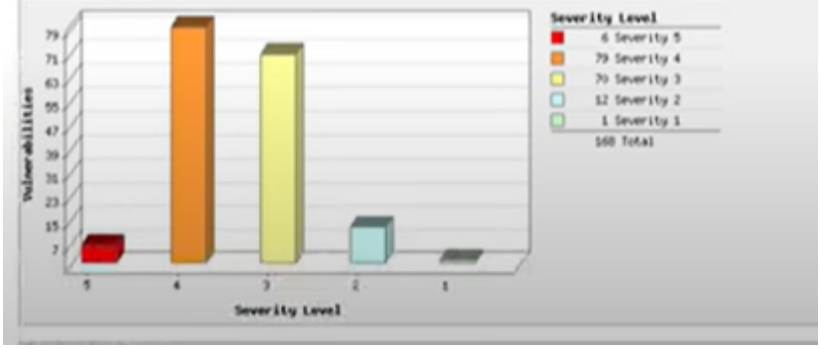
by Severity

Severity	Confirmed	Potential
5	6	0
4	79	0
3	70	0
2	12	4
1	1	0
Total	168	4

5 Biggest Categories

Category	Confirmed	Potential
Local	132	0
Security Policy	6	2
Information gathering	0	2
Windows	28	0
TCP/IP	0	0
Total	166	4

Vulnerabilities by Severity



Vulnerabilities (117)

- 5 Microsoft Edge Based on Chromium Prior to 94.0.992.31 Multiple Vulnerabilities
- 5 VideoLAN VLC Media player Stack smashing in SMB/CIFS access (VideoLAN-SA-1006)
- 5 Microsoft Edge Based on Chromium Prior to 107.0.1418.42 Multiple Vulnerabilities

QID: 377757
Category: Local
Associated CVEs: CVE-2022-3887 CVE-2022-3885 CVE-2022-3888 CVE-2022-3886 CVE-2022-3889 CVE-2022-3890
Vendor Reference Edge (chromium based) 107.0.1418.42
Bugtraq ID: -
Service Modified: 12/01/2022
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.
QID Detection Logic: (Authenticated).
It checks package versions to check for the vulnerable packages.

Note: The preceding description block is extracted directly from the security advisory. Using automation, we have attempted to clean and format it as much as possible without in issues.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 107.0.1418.42 or later
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Edge (chromium based) 107.0.1418.42

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

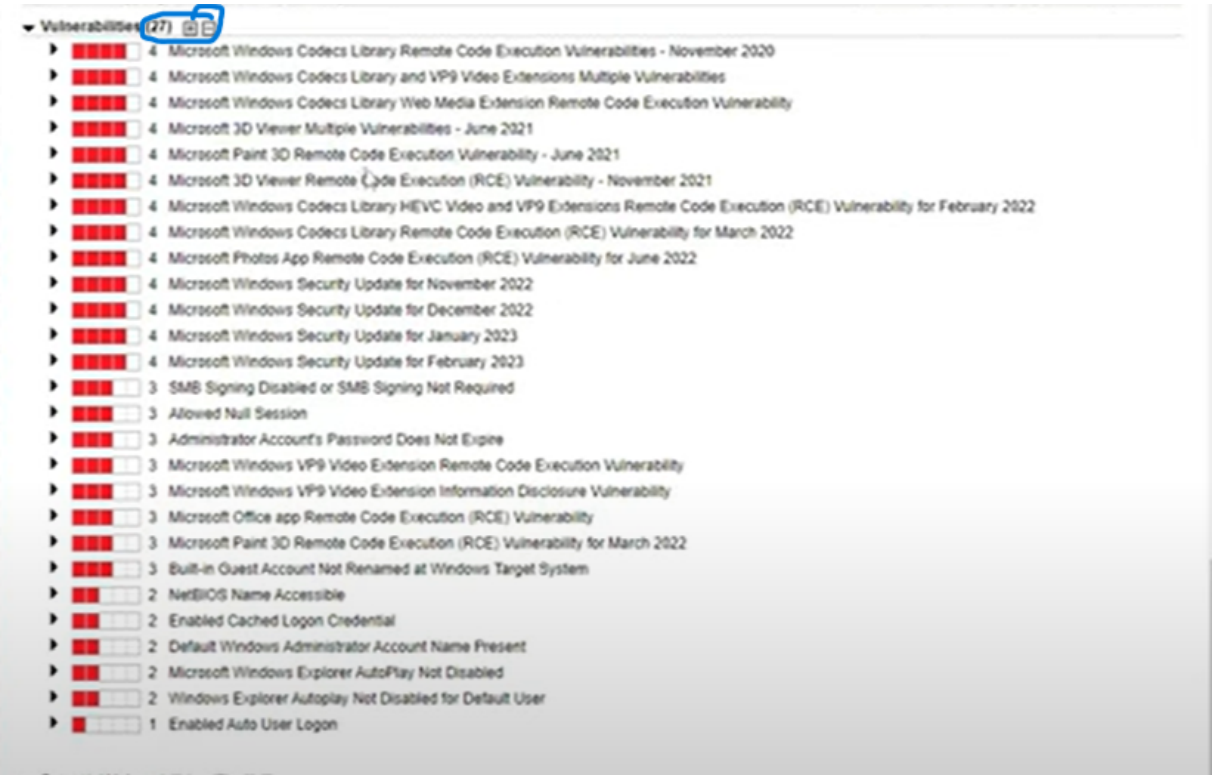
ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 92.0.902.67

- Leveraged Qualys to decrease the vulnerabilities from 117 down to 27 by updating windows and removing outdated software, verified the vulnerabilities were no longer present by rescanning the network.
    - ☐ Detected outdated Windows 10 machine, remediated the vulnerabilities, verified the software was no longer vulnerable.



- In this lab I used Qualys scanner. I introduced a Vulnerability Management strategy Discover, Prioritize, Asses, Report, Remediate,Verify to deal with vulnerabilities stemming from old versions of windows as well as third party software, in this case it was firefox and VLC media player. In this lab, I removed over 80 vulnerabilities on the network optimizing the Qualys scanner to identify security flaws on important systems.