External Vulnerabilities by Issue – Detail Alert

Issue 1: jQuery End of Life (EOL) Detection (Linux) (CVSS: 9.9)
Summary: The installed version of jQuery on the remote host has reached the End of Life (EOL) and should not be used anymore.
Solution: Update jQuery on the remote host to a still supported version.
Affected Nodes: External 96-67-119-198-static.hfc.comcastbusiness.net (96.67.119.198)

Issue 2: Dnsmasq <= 2.86 Multiple Vulnerabilities (CVSS: 9.8)
Summary: Dnsmasq is prone to multiple vulnerabilities.
Solution: No known solution is available as of 11th January, 2022. Information regarding this issue will be updated once solution details are available.
Affected Nodes: External 96-67-119-198-static.hfc.comcastbusiness.net (96.67.119.198)

Issue 3: Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux (CVSS: 9.8)
Summary: Apache HTTP Server is prone to a buffer overflow vulnerability.
Solution: Update to version 2.4.52 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 4: Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 5: Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.30 or later. Please see the references for more information.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 6: Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.49 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 7: Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.

Solution: Update to version 2.4.48 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 8: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux) (CVSS: 9.8)
Summary: openssh is prone to a security bypass vulnerability.
Solution: Upgrade to OpenSSH version 7.2 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 9: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.53 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 10: Apache HTTP Server mod_auth_digest Multiple Vulnerabilities (Linux) (CVSS: 9.1)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 11: OpenSSH Multiple Vulnerabilities (CVSS: 8.5)
Summary: OpenSSH is prone to multiple vulnerabilities.
Solution: Upgrade to OpenSSH 7.0 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 12: Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Linux (CVSS: 8.2)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.52 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 13: Dnsmasq < 2.83 Multiple Vulnerabilities (DNSpooq) (CVSS: 8.1)
Summary: Dnsmasq is prone to multiple vulnerabilities dubbed 'DNSpooq'.
Solution: Update to version 2.83 or later.
Affected Nodes: External 96-67-119-198-static.hfc.comcastbusiness.net (96.67.119.198)

Issue 14: OpenSSH Client Information Leak (CVSS: 8.1)
Summary: The OpenSSH client code between 5.4 and 7.1p1 contains experimental support for resuming SSH-connections (roaming). The matching server code has never been shipped, but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server, including private client user keys. The authentication of the server host key prevents exploitation by a man-in-the-middle, so

this information leak is restricted to connections to malicious or compromised servers.
Solution: Update to 7.1p2 or newer.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 15: Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux) (CVSS: 8.1)
Summary: Apache HTTP Server is prone to a man-in-the-middle attack vulnerability.
Solution: Update to version 2.4.24, or 2.2.32, or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 16: OpenSSH <= 8.6 Command Injection Vulnerability (CVSS: 7.8)
Summary: OpenSSH is prone to a remote code execution vulnerability.
Solution: No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 17: OpenSSH Privilege Escalation Vulnerability - May16 (CVSS: 7.8)
Summary: openssh is prone to a privilege escalation vulnerability.
Solution: Upgrade to OpenSSH version 7.2p2-3 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)

Issue 18: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) (CVSS: 7.5)
Summary: The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.
Solution: '- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.
Affected Nodes: External 96-67-119-198-static.hfc.comcastbusiness.net (96.67.119.198), 96-67-119-196-static.hfc.comcastbusiness.net (96.67.119.196)

Issue 19: Dnsmasq <= 2.78 DNSSEC Vulnerability (CVSS: 7.5)
Summary: Dnsmasq is prone to an improper DNSSEC validation vulnerability.
Solution: Update to version 2.79 or later.
Affected Nodes: External 96-67-119-198-static.hfc.comcastbusiness.net (96.67.119.198)

Issue 20: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux) (CVSS: 7.5)

Summary: openssh is prone to denial of service and user enumeration vulnerabilities.
Solution: Upgrade to OpenSSH version 7.3 or later.
Affected Nodes: External scanme.nmap.org (45.33.32.156)