External Vulnerabilities by Device - Alert

IP: scanme.nmap.org (45.33.32.156)
Issue 1: Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux (CVSS: 9.8)
Issue 2: Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (CVSS: 9.8)
Issue 3: Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (CVSS: 9.8)
Issue 4: Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Issue 5: Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Issue 6: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux) (CVSS: 9.8)
Issue 7: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Issue 8: Apache HTTP Server mod_auth_digest Multiple Vulnerabilities (Linux) (CVSS: 9.1)
Issue 9: OpenSSH Multiple Vulnerabilities (CVSS: 8.5)
Issue 10: Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Linux (CVSS: 8.2)
Issue 11: OpenSSH Client Information Leak (CVSS: 8.1)
Issue 12: Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux) (CVSS: 8.1)
Issue 13: OpenSSH <= 8.6 Command Injection Vulnerability (CVSS: 7.8)
Issue 14: OpenSSH Privilege Escalation Vulnerability - May16 (CVSS: 7.8)
Issue 15: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux) (CVSS: 7.5)
Issue 16: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater) (CVSS: 7.5)
Issue 17: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux) (CVSS: 7.5)
Issue 18: Apache HTTP Server mod_auth_digest DoS Vulnerability (Linux) (CVSS: 7.5)
Issue 19: Apache HTTP Server Whitespace Defects Multiple Vulnerabilities (CVSS: 7.5)
Issue 20: Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux (CVSS: 7.5)
Issue 21: Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux) (CVSS: 7.5)
Issue 22: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux) (CVSS: 7.5)
Issue 23: Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux (CVSS: 7.5)
Issue 24: Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check (CVSS: 7.5)
Issue 25: OpenSSH Multiple Vulnerabilities Jan17 (Linux) (CVSS: 7.3)
Issue 26: OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability (CVSS: 7)
Issue 27: Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux (CVSS: 6.8)
Issue 28: Apache HTTP Server Multiple Vulnerabilities May15 (CVSS: 6.8)
Issue 29: OpenSSH <= 7.2p1 - Xauth Injection (CVSS: 6.4)
Issue 30: Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux) (CVSS: 6.1)
Issue 31: Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux (CVSS: 6.1)
Issue 32: Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux) (CVSS: 6.1)
Issue 33: OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145) (CVSS: 5.9)
Issue 34: OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities (CVSS: 5.9)
Issue 35: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) (CVSS: 5.3)
Issue 36: OpenSSH auth2-gss.c User Enumeration Vulnerability - Linux (CVSS: 5.3)
Issue 37: Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux) (CVSS: 5.3)
Issue 38: OpenSSH Denial of Service Vulnerability - Jan16 (CVSS: 5.3)
Issue 39: Weak Host Key Algorithm(s) (SSH) (CVSS: 5.3)

Issue 40: Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux) (CVSS: 5.3)
Issue 41: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) (CVSS: 5.3)
Issue 42: Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux (CVSS: 5.3)
Issue 43: OpenSSH < 7.8 User Enumeration Vulnerability - Linux (CVSS: 5.3)
Issue 44: OpenSSH sftp-server Security Bypass Vulnerability (Linux) (CVSS: 5.3)
Issue 45: Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux (CVSS: 5)
Issue 46: Apache HTTP Server Multiple Vulnerabilities August15 (Linux) (CVSS: 5)
Issue 47: Enabled Directory Listing Detection (CVSS: 5)
Issue 48: Apache HTTP Server mod_lua Denial of Service Vulnerability -01 May15 (CVSS: 5)
Issue 49: Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux (CVSS: 5)
Issue 50: Apache HTTP Server mod_lua Denial of Service Vulnerability May15 (CVSS: 4.3)
Issue 51: Apache HTTP Server mod_cache Denial of Service Vulnerability -01 May15 (CVSS: 4.3)
Issue 52: Weak Encryption Algorithm(s) Supported (SSH) (CVSS: 4.3)
Issue 53: OpenSSH Security Bypass Vulnerability (CVSS: 4.3)
Issue 54: TCP timestamps (CVSS: 2.6)
Issue 55: Weak MAC Algorithm(s) Supported (SSH) (CVSS: 2.6)

IP: 96-67-119-196-static.hfc.comcastbusiness.net (96.67.119.196)
Issue 1: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) (CVSS: 7.5)
Issue 2: SSL/TLS: Missing `secure` Cookie Attribute (CVSS: 6.4)
Issue 3: SSL/TLS: BREACH attack against HTTP compression (CVSS: 5.9)
Issue 4: SSL/TLS: Certificate Expired (CVSS: 5)
Issue 5: Missing `httpOnly` Cookie Attribute (CVSS: 5)
Issue 6: TCP timestamps (CVSS: 2.6)

IP: 96-67-119-198-static.hfc.comcastbusiness.net (96.67.119.198)
Issue 1: jQuery End of Life (EOL) Detection (Linux) (CVSS: 9.9)
Issue 2: Dnsmasq <= 2.86 Multiple Vulnerabilities (CVSS: 9.8)
Issue 3: Dnsmasq < 2.83 Multiple Vulnerabilities (DNSpooq) (CVSS: 8.1)
Issue 4: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) (CVSS: 7.5)
Issue 5: Dnsmasq <= 2.78 DNSSEC Vulnerability (CVSS: 7.5)
Issue 6: jQuery 1.2 < 3.5.0 XSS Vulnerability (CVSS: 6.1)
Issue 7: jQuery 1.0.3 < 3.5.0 XSS Vulnerability (CVSS: 6.1)
Issue 8: jQuery 1.4.2 <= 1.11.0 XSS Vulnerability (CVSS: 6.1)
Issue 9: jQuery < 3.4.0 Object Extensions Vulnerability (CVSS: 6.1)
Issue 10: jQuery < 3.0.0 XSS Vulnerability (CVSS: 6.1)
Issue 11: SSL/TLS: Certificate Expired (CVSS: 5)
Issue 12: Backup File Scanner (HTTP) - Unreliable Detection Reporting (CVSS: 5)
Issue 13: Cleartext Transmission of Sensitive Information via HTTP (CVSS: 4.8)
Issue 14: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (CVSS: 4.3)
Issue 15: Dnsmasq < 2.85 DNS Cache Poisoning Vulnerability (CVSS: 4)
Issue 16: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (CVSS: 4)

Issue 17: Dnsmasq < 2.81 DoS Vulnerability (CVSS: 3.7)
Issue 18: TCP timestamps (CVSS: 2.6)