My Basic Network Scan

Report generated by Nessus™ Wed, 08 Mar 2023 16:33:17 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.16.128

Vulnerabilities Total: 72

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	7.4	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	6.7	11915	Apache < 1.3.29 Multiple Modules Local Overflow
CRITICAL	9.8	7.4	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	-	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.0	7.3	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	78555	OpenSSL Unsupported
CRITICAL	10.0*	5.8	15555	Apache mod_proxy Content-Length Overflow
CRITICAL	10.0*	5.9	17757	OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities
HIGH	7.5	5.1	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	5.9	31654	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow
HIGH	7.5*	5.3	13651	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String
HIGH	9.3*	5.9	17760	OpenSSL < 0.9.8f Multiple Vulnerabilities
HIGH	9.3*	5.9	57459	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	7.5*	6.7	58799	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption

HIGH	7.5*	5.5	12255	mod_ssl ssl_util_uuencode_binary Remote Overflow
MEDIUM	6.8	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	3.3	17696	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	5.1	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	1.4	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	5.0*	4.4	12280	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS
MEDIUM	5.0*	5.9	59076	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service
MEDIUM	5.0*	4.4	17750	OpenSSL < 0.9.6m / 0.9.7d Denial of Service
MEDIUM	5.0*	4.4	12110	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS
MEDIUM	5.0*	3.4	17755	OpenSSL < 0.9.7h / 0.9.8a Protocol Version Rollback
MEDIUM	4.3*	3.5	17756	OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability
MEDIUM	5.0*	3.4	17759	OpenSSL < 0.9.8 Weak Default Configuration
MEDIUM	4.3*	4.2	56996	OpenSSL < 0.9.8h Multiple Vulnerabilities
MEDIUM	5.0*	5.1	17761	OpenSSL < 0.9.8i Denial of Service
MEDIUM	5.8*	4.0	17762	OpenSSL < 0.9.8j Signature Spoofing
MEDIUM	5.0*	3.6	17763	OpenSSL < 0.9.8k Multiple Vulnerabilities
MEDIUM	5.1*	6.7	17765	OpenSSL < 0.9.8l Multiple Vulnerabilities

MEDIUM	5.0*	3.6	58564	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	5.8*	7.7	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.9	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.1*	2.7	17754	OpenSSL < 0.9.7f Insecure Temporary File Creation
LOW	2.6*	3.6	64532	OpenSSL < 0.9.8y Multiple Vulnerabilities
LOW	N/A	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	57323	OpenSSL Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported

INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	53360	SSL Server Accepts Weak Diffie-Hellman Keys
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown