Basic Vulnerability Scan

Report generated by Tenable Nessus™ Wed, 17 Sep 2025 15:34:38 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

[redacted]

Vulnerabilities Total: 95

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.9	0.489	58327	Samba 'AndX' Request Heap-Based Buffer Overflow
HIGH	7.5	6.7	0.9173	71783	Network Time Protocol Daemon (ntpd) monlist Command Ena DoS
HIGH	7.5	6.1	0.2879	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.7865	90509	Samba Badlock Vulnerability
HIGH	7.5*	7.4	0.9432	78515	Drupal Database Abstraction API SQLi
HIGH	7.5*	5.2	0.9233	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	7.3	0.904	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.8	-	-	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.3	5.9	0.0032	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	-	-	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	4.0	0.524	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	4.2	0.0815	35291	SSL Certificate Signed Using Weak Hashing Algorithm

MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	6.4*	3.6	0.8693	43156	NTP ntpd Mode 7 Error Response Packet Loop Remote DoS
MEDIUM	4.0*	7.3	0.6945	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	5.0*	4.4	0.0787	76474	SNMP 'GETBULK' Reflection DDoS
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	1.4	0.9191	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE
MEDIUM	5.0*	-	-	12218	mDNS Detection (Remote Network)
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	0.9391	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	0.9391	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	3.4	5.1	0.9377	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
LOW	2.6*	-	-	10407	X Server Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	18638	Drupal Software Detection

INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
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	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	14274	Nessus SNMP Scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	57323	OpenSSL Version Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	35296	SNMP Protocol Version Detection
INFO	N/A	-	-	34022	SNMP Query Routing Information Disclosure
INFO	N/A	-	-	10550	SNMP Query Running Process List Disclosure

INFO	N/A	-	-	10800	SNMP Query System Information Disclosure
INFO	N/A	-	-	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	-	185519	SNMP Server Detection
INFO	N/A	-	-	40448	SNMP Supported Protocols Detection
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
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	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval

INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	32318	Web Site Cross-Domain Policy File Detection
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

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