Patrick_Oliver_Custom_DC

Report generated by Nessus™ Fri, 08 Sep 2023 20:43:02 AEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

172.16.1.36

Vulnerabilities Total: 37

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	70658	SSH Server CBC Mode Ciphers Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	70657	SSH Algorithms and Languages Supported

INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
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	-	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	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
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

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

172.16.1.50

Vulnerabilities Total: 120

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	181128	Microsoft Edge (Chromium) < 116.0.1938.76 Multiple Vulnerabilities
CRITICAL	9.6	-	180174	WinRAR < 6.23 RCE
HIGH	7.8	-	180360	7-Zip < 23.00 Multiple Vulnerabilities
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.4	-	166555	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
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	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	91231	7-Zip Installed
INFO	N/A	-	92415	Application Compatibility Cache
INFO	N/A	-	34096	BIOS Info (WMI)
INFO	N/A	-	24270	Computer Manufacturer Information (WMI)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	139785	DISM Package List (Windows)
INFO	N/A	-	55472	Device Hostname

INFO	N/A	-	71246	Enumerate Local Group Memberships
INFO	N/A	-	72684	Enumerate Users via WMI
INFO	N/A	-	168980	Enumerate the PATH Variables
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	171410	IP Assignment Method Detection
INFO	N/A	-	179947	Intel CPUID detection
INFO	N/A	-	92421	Internet Explorer Typed URLs
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	92424	MUICache Program Execution History
INFO	N/A	-	51351	Microsoft .NET Framework Detection
INFO	N/A	-	176212	Microsoft Edge Add-on Enumeration (Windows)
INFO	N/A	-	136969	Microsoft Edge Chromium Installed
INFO	N/A	-	72879	Microsoft Internet Explorer Enhanced Security Configuration Detection
INFO	N/A	-	72367	Microsoft Internet Explorer Version Detection
INFO	N/A	-	125835	Microsoft Remote Desktop Connection Installed
INFO	N/A	-	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	-	48763	Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting
INFO	N/A	-	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	-	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
INFO	N/A	-	10916	Microsoft Windows - Local Users Information : Passwords Never Expire

INFO	N/A	-	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	-	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	-	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	-	10900	Microsoft Windows - Users Information : Passwords Never Expire
INFO	N/A	-	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	-	92370	Microsoft Windows ARP Table
INFO	N/A	-	92371	Microsoft Windows DNS Cache
INFO	N/A	-	92364	Microsoft Windows Environment Variables
INFO	N/A	-	92365	Microsoft Windows Hosts File
INFO	N/A	-	20811	Microsoft Windows Installed Software Enumeration (credentialed check)
INFO	N/A	-	178102	Microsoft Windows Installed Software Version Enumeration
INFO	N/A	-	161502	Microsoft Windows Logged On Users
INFO	N/A	-	63080	Microsoft Windows Mounted Devices
INFO	N/A	-	92372	Microsoft Windows NetBIOS over TCP/IP Info
INFO	N/A	-	103871	Microsoft Windows Network Adapters
INFO	N/A	-	92367	Microsoft Windows PowerShell Execution Policy
INFO	N/A	-	70329	Microsoft Windows Process Information
INFO	N/A	-	70331	Microsoft Windows Process Module Information
INFO	N/A	-	34252	Microsoft Windows Remote Listeners Enumeration (WMI)
INFO	N/A	-	126527	Microsoft Windows SAM user enumeration
INFO	N/A	-	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	-	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
INFO	N/A	-	10400	Microsoft Windows SMB Registry Remotely Accessible
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	10456	Microsoft Windows SMB Service Enumeration
INFO	N/A	-	92373	Microsoft Windows SMB Sessions
INFO	N/A	-	23974	Microsoft Windows SMB Share Hosting Office Files
INFO	N/A	-	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	-	10396	Microsoft Windows SMB Shares Access
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	92368	Microsoft Windows Scripting Host Settings
INFO	N/A	-	58452	Microsoft Windows Startup Software Enumeration
INFO	N/A	-	92369	Microsoft Windows Time Zone Information
INFO	N/A	-	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	-	64582	Netstat Connection Information
INFO	N/A	-	34220	Netstat Portscanner (WMI)
INFO	N/A	-	24272	Network Interfaces Enumeration (WMI)
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	139241	Python Software Foundation Python Installed (Windows)
INFO	N/A	-	122422	RARLAB WinRAR Installed (Windows)
INFO	N/A	-	92428	Recent File History
INFO	N/A	-	92429	Recycle Bin Files
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection

INFO	N/A	-	62042	SMB QuickFixEngineering (QFE) Enumeration
INFO	N/A	-	10860	SMB Use Host SID to Enumerate Local Users
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	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	56468	Time of Last System Startup
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	92434	User Download Folder Files
INFO	N/A	-	92431	User Shell Folders Settings
INFO	N/A	-	92435	UserAssist Execution History
INFO	N/A	-	24269	WMI Available
INFO	N/A	-	52001	WMI QuickFixEngineering (QFE) Enumeration
INFO	N/A	-	44871	WMI Windows Feature Enumeration
INFO	N/A	-	33139	WS-Management Server Detection
INFO	N/A	-	92436	WinRAR History
INFO	N/A	-	48337	Windows ComputerSystemProduct Enumeration (WMI)
INFO	N/A	-	58181	Windows DNS Server Enumeration

INFO	N/A	-	164690	Windows Disabled Command Prompt Enumeration
INFO	N/A	-	72482	Windows Display Driver Enumeration
INFO	N/A	-	171956	Windows Enumerate Accounts
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	155963	Windows Printer Driver Enumeration
INFO	N/A	-	63620	Windows Product Key Retrieval
INFO	N/A	-	85736	Windows Store Application Enumeration

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

172.16.1.51

Vulnerabilities Total: 21

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
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	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported

INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	106375	nginx HTTP Server Detection

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

kali.cqu

1	4	7	1	67
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 80

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	126258	Linux Malicious File Detection
HIGH	7.5	-	151905	OpenJDK 7 <= 7u301 / 8 <= 8u292 / 11.0.0 <= 11.0.11 / 13.0.0 <= 13.0.7 / 15.0.0 <= 15.0.3 / 16.0.0 <= 16.0.1 Multiple Vulnerabilities (2021-07-20)
HIGH	7.5	-	159948	OpenJDK 7 <= 7u331 / 8 <= 8u322 / 11.0.0 <= 11.0.14 / 13.0.0 <= 13.0.10 / 15.0.0 <= 15.0.6 / 17.0.0 <= 17.0.2 / 18.0.0 <= 18.0.0 Multiple Vulnerabilities (2022-04-19)
HIGH	7.5	-	163455	OpenJDK 7 <= 7u341 / 8 <= 8u332 / 11.0.0 <= 11.0.15 / 13.0.0 <= 13.0.11 / 15.0.0 <= 15.0.7 / 17.0.0 <= 17.0.3 / 18.0.0 <= 18.0.1 Multiple Vulnerabilities (2022-07-19
HIGH	N/A	-	151209	OpenJDK 7 <= 7u281 / 8 <= 8u272 / 11.0.0 <= 11.0.9 / 13.0.0 <= 13.0.5 / 15.0.0 <= 15.0.1 Vulnerability (2021-01-19)
MEDIUM	6.8	-	154657	OpenJDK 7 <= 7u311 / 8 <= 8u302 / 11.0.0 <= 11.0.12 / 13.0.0 <= 13.0.8 / 15.0.0 <= 15.0.4 / 16.0.0 <= 16.0.2 Multiple Vulnerabilities (2021-10-19
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	180253	Tenable Nessus < 10.6.0 Multiple Vulnerabilities (TNS-2023-29)
MEDIUM	5.9	-	151207	OpenJDK 7 <= 7u291 / 8 <= 8u282 / 11.0.0 <= 11.0.10 / 13.0.0 <= 13.0.6 / 15.0.0 <= 15.0.2 / 16.0.0 Multiple Vulnerabilities (2021-04-20)
MEDIUM	5.3	-	156854	OpenJDK 7 <= 7u321 / 8 <= 8u312 / 11.0.0 <= 11.0.13 / 13.0.0 <= 13.0.9 / 15.0.0 <= 15.0.5 / 17.0.0 <= 17.0.1 Multiple Vulnerabilities (2022-01-18
MEDIUM	5.3	-	166381	OpenJDK 7 <= 7u351 / 8 <= 8u342 / 11.0.0 <= 11.0.16 / 13.0.0 <= 13.0.12 / 15.0.0 <= 15.0.8 / 17.0.0 <= 17.0.4 / 19.0.0 <= 19.0.0 Multiple Vulnerabilities (2022-10-18

MEDIUM	5.3	-	170536	OpenJDK 7 <= 7u361 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <= 15.0.9 / 17.0.0 <= 17.0.5 / 19.0.0 <= 19.0.1 Multiple Vulnerabilities (2023-01-17
LOW	3.1	-	33851	Network daemons not managed by the package system
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	148375	AdoptOpenJDK Java Detection (Linux / Unix)
INFO	N/A	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	156000	Apache Log4j Installed (Linux / Unix)
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	34098	BIOS Info (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	55472	Device Hostname
INFO	N/A	-	54615	Device Type
INFO	N/A	-	159273	Dockerfile Detection for Linux/UNIX
INFO	N/A	-	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	33276	Enumerate MAC Addresses via SSH
INFO	N/A	-	170170	Enumerate the Network Interaface configuration via SSH
INFO	N/A	-	179200	Enumerate the Network Routing configuration via SSH
INFO	N/A	-	168980	Enumerate the PATH Variables
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	168982	Filepaths contain Dangerous characters (Linux)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution

INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	171410	IP Assignment Method Detection
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	147817	Java Detection and Identification (Linux / Unix)
INFO	N/A	-	151883	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	-	157358	Linux Mounted Devices
INFO	N/A	-	95928	Linux User List Enumeration
INFO	N/A	-	130626	MariaDB Client/Server Installed (Linux)
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10147	Nessus Server Detection
INFO	N/A	-	64582	Netstat Connection Information
INFO	N/A	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	117887	OS Security Patch Assessment Available
INFO	N/A	-	148373	OpenJDK Java Detection (Linux / Unix)
INFO	N/A	-	168007	OpenSSL Installed (Linux)
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	130024	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	-	45405	Reachable IPv6 address
INFO	N/A	-	25221	Remote listeners enumeration (Linux / AIX)
INFO	N/A	-	174788	SQLite Local Detection (Linux)
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted

INFO	N/A	-	10881	SSH Protocol Versions Supported
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	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	22869	Software Enumeration (SSH)
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	35351	System Information Enumeration (via DMI)
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110095	Target Credential Issues by Authentication Protocol - No Issues Found
INFO	N/A	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	163326	Tenable Nessus Installed (Linux)
INFO	N/A	-	56468	Time of Last System Startup
INFO	N/A	-	110483	Unix / Linux Running Processes Information
INFO	N/A	-	152742	Unix Software Discovery Commands Available
INFO	N/A	-	136340	nginx Installed (Linux/UNIX)

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