



# EPICODE S5L4

Report generated by Nessus™

Tue, 02 Jan 2024 18:30:55 CET

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.1.100.....	4
• 192.168.1.101.....	7

Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.1.100



## Vulnerabilities

Total: 53

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	182774	Curl Installed (Linux / Unix)
INFO	N/A	-	55472	Device Hostname
INFO	N/A	-	54615	Device Type
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 Interface 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	-	<a href="#">171410</a>	IP Assignment Method Detection
INFO	N/A	-	<a href="#">147817</a>	Java Detection and Identification (Linux / Unix)
INFO	N/A	-	<a href="#">151883</a>	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	-	<a href="#">157358</a>	Linux Mounted Devices
INFO	N/A	-	<a href="#">95928</a>	Linux User List Enumeration
INFO	N/A	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	<a href="#">10147</a>	Nessus Server Detection
INFO	N/A	-	<a href="#">64582</a>	Netstat Connection Information
INFO	N/A	-	<a href="#">14272</a>	Netstat Portscanner (SSH)
INFO	N/A	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	<a href="#">97993</a>	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	<a href="#">117887</a>	OS Security Patch Assessment Available
INFO	N/A	-	<a href="#">148373</a>	OpenJDK Java Detection (Linux / Unix)
INFO	N/A	-	<a href="#">168007</a>	OpenSSL Installed (Linux)
INFO	N/A	-	<a href="#">130024</a>	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	-	<a href="#">45405</a>	Reachable IPv6 address
INFO	N/A	-	<a href="#">174788</a>	SQLite Local Detection (Linux)
INFO	N/A	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	<a href="#">22869</a>	Software Enumeration (SSH)
INFO	N/A	-	<a href="#">42822</a>	Strict Transport Security (STS) Detection
INFO	N/A	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection

INFO	N/A	-	<a href="#">138330</a>	TLS Version 1.3 Protocol Detection
INFO	N/A	-	<a href="#">110095</a>	Target Credential Issues by Authentication Protocol - No Issues Found
INFO	N/A	-	<a href="#">141118</a>	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	<a href="#">163326</a>	Tenable Nessus Installed (Linux)
INFO	N/A	-	<a href="#">56468</a>	Time of Last System Startup
INFO	N/A	-	<a href="#">110483</a>	Unix / Linux Running Processes Information
INFO	N/A	-	<a href="#">152742</a>	Unix Software Discovery Commands Available
INFO	N/A	-	<a href="#">182848</a>	libcurl Installed (Linux / Unix)
INFO	N/A	-	<a href="#">136340</a>	nginx Installed (Linux/UNIX)

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

## 192.168.1.101



### Vulnerabilities

Total: 94

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
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	-	136808	ISC BIND Denial of Service
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

MEDIUM	5.3	-	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	4.3*	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
LOW	3.7	-	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.4	-	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	<a href="#">10407</a>	X Server Detection
INFO	N/A	-	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	<a href="#">10223</a>	RPC portmapper Service Detection
INFO	N/A	-	<a href="#">21186</a>	AJP Connector Detection
INFO	N/A	-	<a href="#">18261</a>	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	-	<a href="#">84574</a>	Backported Security Patch Detection (PHP)
INFO	N/A	-	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	-	<a href="#">39521</a>	Backported Security Patch Detection (WWW)
INFO	N/A	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	<a href="#">10028</a>	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	<a href="#">11002</a>	DNS Server Detection
INFO	N/A	-	<a href="#">35371</a>	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	<a href="#">86420</a>	Ethernet MAC Addresses



INFO	N/A	-	<a href="#">10092</a>	FTP Server Detection
INFO	N/A	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	<a href="#">10397</a>	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	<a href="#">10437</a>	NFS Share Export List
INFO	N/A	-	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	<a href="#">181418</a>	OpenSSH Detection
INFO	N/A	-	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	-	<a href="#">48243</a>	PHP Version Detection
INFO	N/A	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	<a href="#">118224</a>	PostgreSQL STARTTLS Support
INFO	N/A	-	<a href="#">26024</a>	PostgreSQL Server Detection
INFO	N/A	-	<a href="#">22227</a>	RMI Registry Detection
INFO	N/A	-	<a href="#">11111</a>	RPC Services Enumeration
INFO	N/A	-	<a href="#">53335</a>	RPC portmapper (TCP)
INFO	N/A	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	<a href="#">149334</a>	SSH Password Authentication Accepted

INFO	N/A	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	<a href="#">45410</a>	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	<a href="#">62563</a>	SSL Compression Methods Supported
INFO	N/A	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	-	<a href="#">104887</a>	Samba Version
INFO	N/A	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	<a href="#">11819</a>	TFTP Daemon Detection
INFO	N/A	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	<a href="#">11154</a>	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	<a href="#">19288</a>	VNC Server Security Type Detection
INFO	N/A	-	<a href="#">65792</a>	VNC Server Unencrypted Communication Detection
INFO	N/A	-	<a href="#">10342</a>	VNC Software Detection
INFO	N/A	-	<a href="#">135860</a>	WMI Not Available

INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	52703	vsftpd Detection

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