



## Primer escaneo

---

Report generated by Nessus™

Thu, 07 Mar 2024 21:58:16 CST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- 192.168.1.18.....4

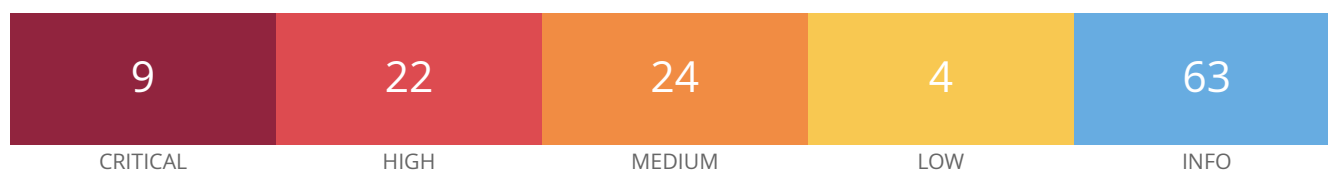
Nessus Essentials

---

## Vulnerabilities by Host

---

192.168.1.18



## Vulnerabilities

Total: 122

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	156860	Apache Log4j 1.x Multiple Vulnerabilities
CRITICAL	9.8	6.7	90888	OpenSSL 1.0.1 < 1.0.1o ASN.1 Encoder Negative Zero Value Handling RCE
CRITICAL	9.8	6.7	89081	OpenSSL 1.0.1 < 1.0.1s Multiple Vulnerabilities (DROWN)
CRITICAL	9.8	6.7	93814	OpenSSL 1.0.1 < 1.0.1u Multiple Vulnerabilities (SWEET32)
CRITICAL	9.8	9.0	182874	libcurl 7.69 < 8.4.0 Heap Buffer Overflow
CRITICAL	9.0	7.3	111162	Oracle Java SE Multiple Vulnerabilities (July 2018 CPU) (Unix)
CRITICAL	9.0	7.3	118227	Oracle Java SE Multiple Vulnerabilities (October 2018 CPU) (Unix)
CRITICAL	10.0	-	182252	Apache Log4j SEoL (<= 1.x)
CRITICAL	10.0	-	64816	Oracle Java JRE Unsupported Version Detection (Unix)
HIGH	8.6	5.5	154381	Azul Zulu Java Multiple Vulnerabilities (2021-10-19)
HIGH	8.6	5.9	154345	Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (Unix October 2021 CPU)
HIGH	8.3	7.3	138576	Oracle Java SE 1.7.0_271 / 1.8.0_261 / 1.11.0_8 / 1.14.0_2 Multiple Vulnerabilities (Jul 2020 CPU)
HIGH	8.2	5.1	90890	OpenSSL 1.0.1 < 1.0.1t Multiple Vulnerabilities
HIGH	7.9	7.9	190856	Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 2024 Security Releases).
HIGH	7.8	6.0	174511	Oracle Java SE Multiple Vulnerabilities (April 2023 CPU)
HIGH	7.5	6.7	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)

HIGH	7.5	5.9	<a href="#">153989</a>	Azul Zulu Java Multiple Vulnerabilities (2021-07-20)
HIGH	7.5	4.4	<a href="#">159902</a>	Azul Zulu Java Multiple Vulnerabilities (2022-04-19)
HIGH	7.5	4.4	<a href="#">163301</a>	Azul Zulu Java Multiple Vulnerabilities (2022-07-19)
HIGH	7.5	6.0	<a href="#">189356</a>	OpenJDK 8 <= 8u392 / 11.0.0 <= 11.0.21 / 17.0.0 <= 17.0.9 / 21.0.0 <= 21.0.1 Multiple Vulnerabilities (2024-01-16)
HIGH	7.5	6.1	<a href="#">73404</a>	OpenSSL 1.0.1 < 1.0.1g Multiple Vulnerabilities (Heartbleed)
HIGH	7.5	6.1	<a href="#">93112</a>	OpenSSL < 1.0.2i Default Weak 64-bit Block Cipher (SWEET32)
HIGH	7.5	4.4	<a href="#">161241</a>	Oracle Java SE Multiple Vulnerabilities (April 2022 CPU)
HIGH	7.5	6.0	<a href="#">189116</a>	Oracle Java SE Multiple Vulnerabilities (January 2024 CPU)
HIGH	7.5	4.4	<a href="#">163304</a>	Oracle Java SE Multiple Vulnerabilities (July 2022 CPU)
HIGH	7.5	4.4	<a href="#">178485</a>	Oracle Java SE Multiple Vulnerabilities (July 2023 CPU)
HIGH	7.4	6.0	<a href="#">174549</a>	Azul Zulu Java Multiple Vulnerabilities (2023-04-18)
HIGH	7.4	6.0	<a href="#">171079</a>	OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities
HIGH	7.4	7.3	<a href="#">109203</a>	Oracle Java SE Multiple Vulnerabilities (April 2018 CPU) (Unix)
HIGH	7.5*	7.7	<a href="#">74364</a>	OpenSSL 1.0.1 < 1.0.1h Multiple Vulnerabilities
HIGH	7.5*	5.9	<a href="#">77088</a>	OpenSSL 1.0.1 < 1.0.1i Multiple Vulnerabilities
MEDIUM	6.5	3.6	<a href="#">84636</a>	OpenSSL 1.0.1 < 1.0.1p Multiple Vulnerabilities
MEDIUM	6.5	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	5.9	4.4	<a href="#">178473</a>	Azul Zulu Java Multiple Vulnerabilities (2023-07-18)
MEDIUM	5.9	3.6	<a href="#">153926</a>	Azul Zulu Java OpenJDK Vulnerability (2021-04-20)
MEDIUM	5.9	3.6	<a href="#">148961</a>	Oracle Java SE 1.7.0_301 / 1.8.0_291 / 1.11.0_11 / 1.16.0_1 Multiple Vulnerabilities (Unix Apr 2021 CPU)
MEDIUM	5.7	-	<a href="#">172180</a>	Potentially Dangerous PATH Variables
MEDIUM	5.3	2.2	<a href="#">158673</a>	Azul Zulu Java Multiple Vulnerabilities (2022-01-18)
MEDIUM	5.3	2.2	<a href="#">166222</a>	Azul Zulu Java Multiple Vulnerabilities (2022-10-18)
MEDIUM	5.3	2.2	<a href="#">170112</a>	Azul Zulu Java Multiple Vulnerabilities (2023-01-17)

MEDIUM	5.3	2.2	<a href="#">183512</a>	Azul Zulu Java Multiple Vulnerabilities (2023-10-17)
MEDIUM	5.3	3.6	<a href="#">87221</a>	OpenSSL 1.0.1 < 1.0.1q Multiple DoS
MEDIUM	5.3	4.4	<a href="#">173260</a>	OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities
MEDIUM	5.3	2.9	<a href="#">178475</a>	OpenSSL 1.1.1 < 1.1.1v Vulnerability
MEDIUM	5.3	2.2	<a href="#">184811</a>	OpenSSL 1.1.1 < 1.1.1x Vulnerability
MEDIUM	5.3	3.3	<a href="#">141801</a>	Oracle Java SE 1.7.0_281 / 1.8.0_271 / 1.11.0_9 / 1.15.0_1 Multiple Vulnerabilities (Oct 2020 CPU)
MEDIUM	5.3	2.2	<a href="#">145219</a>	Oracle Java SE 1.7.0_291 / 1.8.0_281 / 1.11.0_10 / 1.15.0_2 Information Disclosure (Jan 2021 CPU)
MEDIUM	5.3	2.2	<a href="#">156888</a>	Oracle Java SE 1.7.0_331 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities (Unix January 2022 CPU)
MEDIUM	5.3	2.2	<a href="#">170161</a>	Oracle Java SE Multiple Vulnerabilities (January 2023 CPU)
MEDIUM	5.3	2.2	<a href="#">166316</a>	Oracle Java SE Multiple Vulnerabilities (October 2022 CPU)
MEDIUM	5.3	2.2	<a href="#">183295</a>	Oracle Java SE Multiple Vulnerabilities (October 2023 CPU)
MEDIUM	5.8*	5.2	<a href="#">71857</a>	OpenSSL 1.0.1 < 1.0.1f Multiple Vulnerabilities
MEDIUM	5.0*	4.5	<a href="#">80568</a>	OpenSSL 1.0.1 < 1.0.1k Multiple Vulnerabilities (FREAK)
MEDIUM	6.8*	5.2	<a href="#">82032</a>	OpenSSL 1.0.1 < 1.0.1m Multiple Vulnerabilities
MEDIUM	6.8*	5.9	<a href="#">84153</a>	OpenSSL 1.0.1 < 1.0.1n Multiple Vulnerabilities (Logjam)
LOW	3.7	4.5	<a href="#">88529</a>	OpenSSL 1.0.1 < 1.0.1r Multiple Vulnerabilities (Logjam)
LOW	3.7	2.9	<a href="#">182873</a>	libcurl 7.9.1 < 8.4.0 Cookie Injection
LOW	3.4	5.1	<a href="#">78554</a>	OpenSSL 1.0.1 < 1.0.1j Multiple Vulnerabilities (POODLE)
LOW	2.6*	2.2	<a href="#">64620</a>	OpenSSL 1.0.1 < 1.0.1e Information Disclosure
INFO	N/A	-	<a href="#">141394</a>	Apache HTTP Server Installed (Linux)
INFO	N/A	-	<a href="#">156000</a>	Apache Log4j Installed (Linux / Unix)
INFO	N/A	-	<a href="#">148374</a>	Azul Zulu Java Detection (Linux / Unix)
INFO	N/A	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	<a href="#">182774</a>	Curl Installed (Linux / Unix)

INFO	N/A	-	<a href="#">55472</a>	Device Hostname
INFO	N/A	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	<a href="#">159273</a>	Dockerfile Detection for Linux/UNIX
INFO	N/A	-	<a href="#">25203</a>	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	<a href="#">25202</a>	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	<a href="#">33276</a>	Enumerate MAC Addresses via SSH
INFO	N/A	-	<a href="#">170170</a>	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	<a href="#">179200</a>	Enumerate the Network Routing configuration via SSH
INFO	N/A	-	<a href="#">168980</a>	Enumerate the PATH Variables
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="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	<a href="#">24260</a>	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>	Libcrypt 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="#">129056</a>	Microsoft Visual Studio Code Installed (Linux)
INFO	N/A	-	<a href="#">129468</a>	MySQL Server Installed (Linux)
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="#">178771</a>	Node.js Installed (Linux / UNIX)

INFO	N/A	-	<a href="#">178772</a>	Node.js Modules Installed (Linux)
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="#">71463</a>	Oracle Java JRE Premier Support and Extended Support Version Detection (Unix)
INFO	N/A	-	<a href="#">64815</a>	Oracle Java Runtime Environment (JRE) Detection (Unix)
INFO	N/A	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	<a href="#">45405</a>	Reachable IPv6 address
INFO	N/A	-	<a href="#">133964</a>	SELinux Status Check
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="#">83303</a>	Unix / Linux - Local Users Information : Passwords Never Expire
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="#">186361</a>	VMWare Tools or Open VM Tools Installed (Linux)
INFO	N/A	-	<a href="#">182155</a>	WebM Project WebP Image Library Installed (Linux)
INFO	N/A	-	<a href="#">159182</a>	Zoom Installed (Linux)
INFO	N/A	-	<a href="#">182848</a>	libcurl Installed (Linux / Unix)
INFO	N/A	-	<a href="#">66717</a>	mDNS Detection (Local Network)

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