



## Escaneo avanzado

---

Report generated by Tenable Nessus™

Fri, 23 Aug 2024 13:21:22 CEST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.1.34.....	4
• 192.168.1.52.....	12
• 192.168.1.57.....	13
• 192.168.1.88.....	14
• 192.168.1.92.....	16
• 192.168.1.115.....	17
• 192.168.1.132.....	18
• 192.168.1.141.....	19

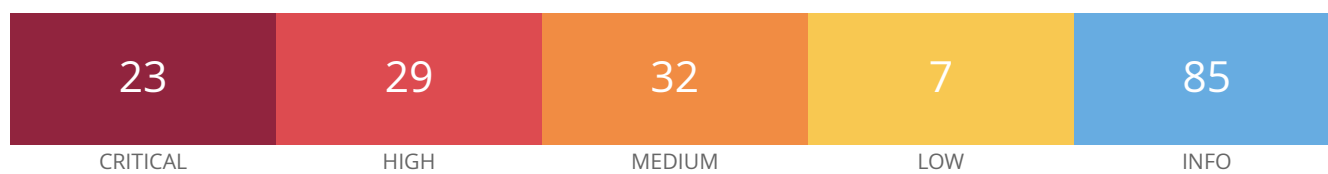
Nessus Essentials

---

## Vulnerabilities by Host

---

192.168.1.34



## Vulnerabilities

Total: 176

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.6684	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.4678	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.3142	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0104	193421	Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL	9.8	6.7	0.019	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0065	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	7.4	0.7374	197839	Apache Tomcat 8.0.0.RC1 < 8.0.39 multiple vulnerabilities
CRITICAL	9.8	6.7	0.0553	111067	Apache Tomcat 8.0.0.RC1 < 8.0.53 multiple vulnerabilities
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	9.7	0.9748	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)
CRITICAL	9.8	8.9	0.4425	73920	SSH Static Key Accepted
CRITICAL	9.1	5.2	0.0147	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0018	197850	Apache Tomcat 8.0.0.RC1 < 8.0.37 multiple vulnerabilities
CRITICAL	9.1	5.2	0.0036	197857	Apache Tomcat 8.0.0.RC1 < 8.0.42
CRITICAL	9.0	6.5	0.0329	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	0.9678	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	-	171356	Apache HTTP Server SEoL (2.1.x <= x <= 2.2.x)
CRITICAL	10.0	-	-	171342	Apache Tomcat SEoL (8.0.x)

CRITICAL	10.0	-	-	<a href="#">58987</a>	PHP Unsupported Version Detection
CRITICAL	10.0	-	-	<a href="#">108797</a>	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.4	0.9746	<a href="#">46740</a>	Apache Axis2 Default Credentials
CRITICAL	10.0*	7.3	0.826	<a href="#">53514</a>	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0*	5.9	0.163	<a href="#">60085</a>	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	8.1	9.2	0.9744	<a href="#">103697</a>	Apache Tomcat 8.0.0.RC1 < 8.0.47
HIGH	8.1	9.8	0.964	<a href="#">97833</a>	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	3.6	0.0064	<a href="#">193422</a>	Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability
HIGH	7.5	3.6	0.3477	<a href="#">193423</a>	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0324	<a href="#">193424</a>	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)
HIGH	7.5	4.4	0.004	<a href="#">183391</a>	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0101	<a href="#">193419</a>	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
HIGH	7.5	5.2	0.0012	<a href="#">192923</a>	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	6.7	0.0004	<a href="#">201532</a>	Apache 2.4.x < 2.4.61
HIGH	7.5	4.4	0.0428	<a href="#">197829</a>	Apache Tomcat 8.0.0.RC1 < 8.0.36
HIGH	7.5	3.6	0.0065	<a href="#">197846</a>	Apache Tomcat 8.0.0.RC1 < 8.0.41
HIGH	7.5	3.6	0.0028	<a href="#">99367</a>	Apache Tomcat 8.0.0.RC1 < 8.0.43
HIGH	7.5	4.4	0.0089	<a href="#">197837</a>	Apache Tomcat 8.0.0.RC1 < 8.0.44
HIGH	7.5	3.6	0.0183	<a href="#">121124</a>	Apache Tomcat 8.0.0.RC1 < 8.0.52
HIGH	7.5	-	-	<a href="#">142591</a>	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	4.2	0.0111	<a href="#">35291</a>	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	5.1	0.0053	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	6.7	0.9558	<a href="#">77531</a>	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities

HIGH	7.3	3.4	0.0035	<a href="#">10547</a>	Microsoft Windows LAN Manager SNMP LanMan Services Disclosure
HIGH	7.3	5.9	0.0179	<a href="#">66584</a>	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities
HIGH	7.3	6.7	0.9498	<a href="#">71426</a>	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities
HIGH	7.3	6.6	0.9481	<a href="#">77285</a>	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.0	5.9	0.0068	<a href="#">62101</a>	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities
HIGH	9.3*	9.6	0.7523	<a href="#">58435</a>	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	7.5*	7.4	0.9372	<a href="#">59056</a>	PHP 5.3.x < 5.3.13 CGI Query String Code Execution
HIGH	7.5*	6.7	0.0946	<a href="#">59529</a>	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities
HIGH	7.5*	5.9	0.0179	<a href="#">64992</a>	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities
HIGH	7.5*	9.0	0.9149	<a href="#">58988</a>	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	5.2	0.4545	<a href="#">41028</a>	SNMP Agent Default Community Name (public)
MEDIUM	6.8	6.0	0.0192	<a href="#">90510</a>	MS16-047: Security Update for SAM and LSAD Remote Protocol (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	4.4	0.0028	<a href="#">106976</a>	Apache Tomcat 8.0.0.RC1 < 8.0.50 multiple vulnerabilities
MEDIUM	6.5	2.5	0.0127	<a href="#">18405</a>	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.5	-	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	<a href="#">157288</a>	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.9	6.1	0.9653	<a href="#">187315</a>	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.9	4.4	0.0054	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.6	3.4	0.9265	<a href="#">68915</a>	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.3	6.6	0.9739	<a href="#">57791</a>	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.3	3.0	0.2178	<a href="#">64912</a>	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	5.3	1.4	0.2239	<a href="#">73405</a>	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities

MEDIUM	5.3	1.4	0.0016	<a href="#">193420</a>	Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)
MEDIUM	5.3	-	-	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	-	-	<a href="#">40984</a>	Browsable Web Directories
MEDIUM	5.3	4.0	0.0465	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	3.4	0.0035	<a href="#">10546</a>	Microsoft Windows LAN Manager SNMP LanMan Users Disclosure
MEDIUM	5.3	-	-	<a href="#">152853</a>	PHP < 7.3.28 Email Header Injection
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	1.4	0.0028	<a href="#">102588</a>	Apache Tomcat 8.0.0.RC1 < 8.0.45
MEDIUM	4.0	-	-	<a href="#">58453</a>	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	5.0*	3.6	0.0547	<a href="#">66842</a>	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities
MEDIUM	6.8*	5.9	0.6144	<a href="#">67259</a>	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	0.0248	<a href="#">58966</a>	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	0.0029	<a href="#">73289</a>	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	5.0*	-	-	<a href="#">46803</a>	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	-	<a href="#">57690</a>	Terminal Services Encryption Level is Medium or Low
MEDIUM	4.3*	-	-	<a href="#">85582</a>	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	5.0*	-	-	<a href="#">90067</a>	WordPress User Enumeration
LOW	3.7	1.4	0.002	<a href="#">159462</a>	Apache Tomcat 8.x < 8.5.78 Spring4Shell CVE-2021-43980
LOW	3.7	2.9	0.9736	<a href="#">83875</a>	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.1*	4.2	0.8808	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	<a href="#">30218</a>	Terminal Services Encryption Level is not FIPS-140 Compliant
LOW	N/A	-	-	<a href="#">42057</a>	Web Server Allows Password Auto-Completion
LOW	2.6*	-	-	<a href="#">26194</a>	Web Server Transmits Cleartext Credentials

LOW	2.6*	-	-	<a href="#">34850</a>	Web Server Uses Basic Authentication Without HTTPS
INFO	N/A	-	-	<a href="#">21186</a>	AJP Connector Detection
INFO	N/A	-	-	<a href="#">46180</a>	Additional DNS Hostnames
INFO	N/A	-	-	<a href="#">46739</a>	Apache Axis2 Detection
INFO	N/A	-	-	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	-	-	<a href="#">39446</a>	Apache Tomcat Detection
INFO	N/A	-	-	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	<a href="#">42799</a>	Broken Web Servers
INFO	N/A	-	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	-	<a href="#">10736</a>	DCE Services Enumeration
INFO	N/A	-	-	<a href="#">84239</a>	Debugging Log Report
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="#">49704</a>	External URLs
INFO	N/A	-	-	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	-	<a href="#">12053</a>	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	<a href="#">53513</a>	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	<a href="#">26917</a>	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
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="#">50344</a>	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	-	<a href="#">50345</a>	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	-	<a href="#">14274</a>	Nessus SNMP Scanner
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">24786</a>	Nessus Windows Scan Not Performed with Admin Privileges
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="#">40665</a>	Protected Web Page Detection
INFO	N/A	-	-	<a href="#">66173</a>	RDP Screenshot
INFO	N/A	-	-	<a href="#">10940</a>	Remote Desktop Protocol Service Detection
INFO	N/A	-	-	<a href="#">35296</a>	SNMP Protocol Version Detection
INFO	N/A	-	-	<a href="#">19763</a>	SNMP Query Installed Software Disclosure
INFO	N/A	-	-	<a href="#">34022</a>	SNMP Query Routing Information Disclosure
INFO	N/A	-	-	<a href="#">10550</a>	SNMP Query Running Process List Disclosure
INFO	N/A	-	-	<a href="#">10800</a>	SNMP Query System Information Disclosure
INFO	N/A	-	-	<a href="#">10551</a>	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	-	<a href="#">185519</a>	SNMP Server Detection
INFO	N/A	-	-	<a href="#">40448</a>	SNMP Supported Protocols Detection
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="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	<a href="#">94761</a>	SSL Root Certification Authority Certificate Information
INFO	N/A	-	-	<a href="#">51891</a>	SSL Session Resume Supported
INFO	N/A	-	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	-	<a href="#">11153</a>	Service Detection (HELP Request)
INFO	N/A	-	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	-	<a href="#">121010</a>	TLS Version 1.1 Protocol Detection
INFO	N/A	-	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	<a href="#">64814</a>	Terminal Services Use SSL/TLS
INFO	N/A	-	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	-	<a href="#">85601</a>	Web Application Cookies Not Marked HttpOnly

INFO	N/A	-	-	<a href="#">85602</a>	Web Application Cookies Not Marked Secure
INFO	N/A	-	-	<a href="#">91815</a>	Web Application Sitemap
INFO	N/A	-	-	<a href="#">20108</a>	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	<a href="#">11032</a>	Web Server Directory Enumeration
INFO	N/A	-	-	<a href="#">49705</a>	Web Server Harvested Email Addresses
INFO	N/A	-	-	<a href="#">11419</a>	Web Server Office File Inventory
INFO	N/A	-	-	<a href="#">11422</a>	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	<a href="#">10662</a>	Web mirroring
INFO	N/A	-	-	<a href="#">11424</a>	WebDAV Detection
INFO	N/A	-	-	<a href="#">24004</a>	WebDAV Directory Enumeration
INFO	N/A	-	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	<a href="#">18297</a>	WordPress Detection
INFO	N/A	-	-	<a href="#">101841</a>	WordPress Outdated Plugin Detection
INFO	N/A	-	-	<a href="#">101842</a>	WordPress Plugin Detection

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

192.168.1.52



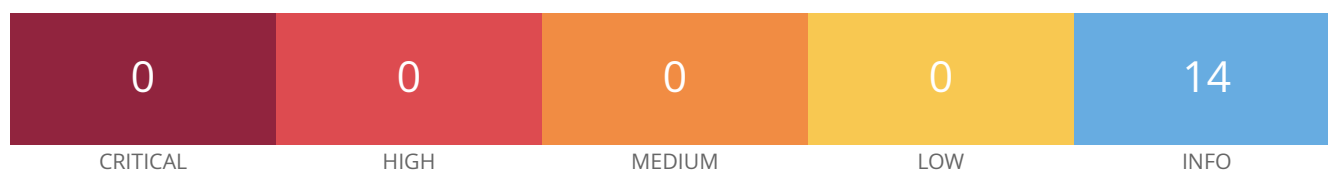
## Vulnerabilities

Total: 9

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

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

192.168.1.57



## Vulnerabilities

Total: 14

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10335	Nessus TCP scanner
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	11865	SOCKS Server Detection
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

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

192.168.1.88



## Vulnerabilities

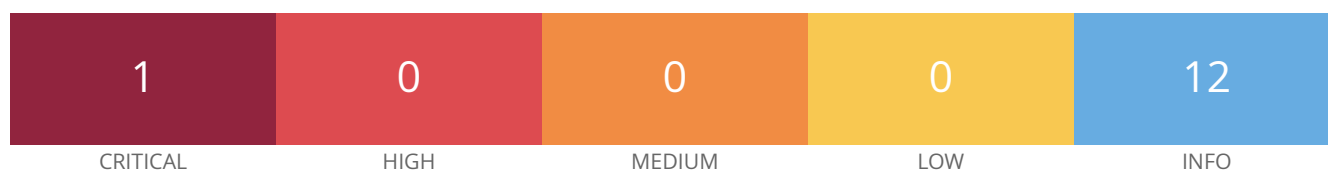
Total: 32

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	19689	Embedded Web Server Detection
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10335	Nessus TCP scanner
INFO	N/A	-	-	11936	OS Identification
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	-	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	<a href="#">94761</a>	SSL Root Certification Authority Certificate Information
INFO	N/A	-	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
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="#">84821</a>	TLS ALPN Supported Protocol Enumeration
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="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">10829</a>	UPnP Client Detection
INFO	N/A	-	-	<a href="#">35711</a>	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	-	<a href="#">11032</a>	Web Server Directory Enumeration
INFO	N/A	-	-	<a href="#">35712</a>	Web Server UPnP Detection

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

192.168.1.92



## Vulnerabilities

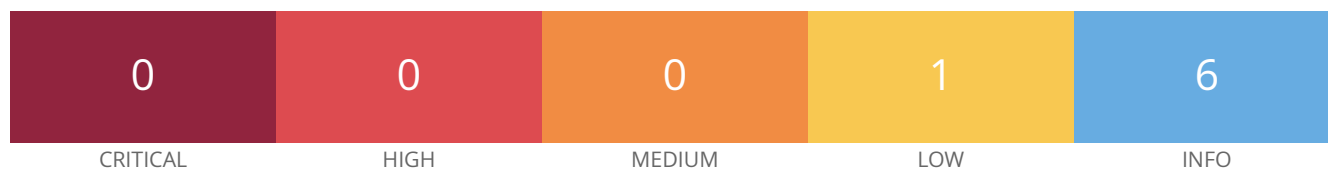
Total: 13

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	0.9742	64394	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE
INFO	N/A	-	-	46180	Additional DNS Hostnames
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	-	35712	Web Server UPnP Detection

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



192.168.1.115



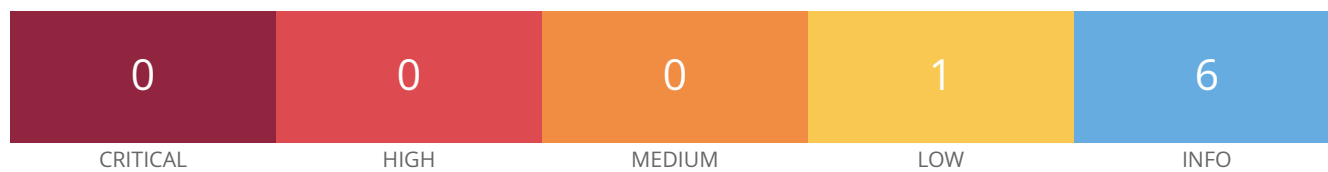
#### Vulnerabilities

Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	10287	Traceroute Information

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

192.168.1.132



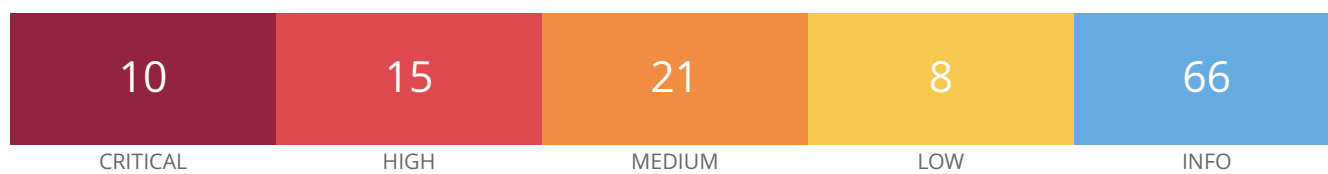
## Vulnerabilities

Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	10287	Traceroute Information

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

192.168.1.141



## Vulnerabilities

Total: 120

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.8	0.975	81510	PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)
CRITICAL	9.8	8.8	0.9533	82025	PHP 5.4.x < 5.4.39 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.6149	83033	PHP 5.4.x < 5.4.40 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.74	83517	PHP 5.4.x < 5.4.41 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0758	84362	PHP 5.4.x < 5.4.42 Multiple Vulnerabilities
CRITICAL	9.8	5.9	0.0203	84671	PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)
CRITICAL	9.8	7.4	0.9709	84215	ProFTPD mod_copy Information Disclosure
CRITICAL	9.8	5.9	0.0101	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	10.0	-	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0*	-	-	92626	Drupal Coder Module Deserialization RCE
HIGH	7.5	-	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	5.9	0.0179	66585	PHP 5.4.x < 5.4.13 Information Disclosure
HIGH	7.3	5.9	0.6144	69401	PHP 5.4.x < 5.4.19 Multiple Vulnerabilities
HIGH	7.3	6.7	0.8801	81080	PHP 5.4.x < 5.4.37 Multiple Vulnerabilities
HIGH	7.3	3.6	0.0219	85298	PHP 5.4.x < 5.4.44 Multiple Vulnerabilities
HIGH	7.3	6.7	0.2011	85885	PHP 5.4.x < 5.4.45 Multiple Vulnerabilities
HIGH	7.5*	7.4	0.9749	78515	Drupal Database Abstraction API SQLi
HIGH	7.5*	5.9	0.0004	26919	Microsoft Windows SMB Guest Account Local User Access

HIGH	9.3*	-	-	<a href="#">67260</a>	PHP 5.4.x < 5.4.17 Buffer Overflow
HIGH	7.5*	6.7	0.9498	<a href="#">71427</a>	PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption
HIGH	7.2*	6.7	0.0004	<a href="#">73862</a>	PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escal
HIGH	7.5*	6.6	0.9481	<a href="#">76281</a>	PHP 5.4.x < 5.4.30 Multiple Vulnerabilities
HIGH	7.5*	6.7	0.9374	<a href="#">78545</a>	PHP 5.4.x < 5.4.34 Multiple Vulnerabilities
HIGH	7.5*	6.6	0.8611	<a href="#">80330</a>	PHP 5.4.x < 5.4.36 'process_nested_data' RCE
MEDIUM	6.5	4.0	0.0035	<a href="#">50686</a>	IP Forwarding Enabled
MEDIUM	6.5	-	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	<a href="#">157288</a>	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.9	6.1	0.9653	<a href="#">187315</a>	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.3	-	-	<a href="#">40984</a>	Browsable Web Directories
MEDIUM	5.3	1.4	0.0016	<a href="#">64993</a>	PHP 5.4.x < 5.4.12 Information Disclosure
MEDIUM	5.3	-	-	<a href="#">152853</a>	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.0*	3.6	0.0547	<a href="#">66843</a>	PHP 5.4.x < 5.4.16 Multiple Vulnerabilities
MEDIUM	5.0*	4.4	0.5897	<a href="#">71927</a>	PHP 5.4.x < 5.4.24 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	0.9586	<a href="#">72881</a>	PHP 5.4.x < 5.4.26 Multiple Vulnerabilities
MEDIUM	5.0*	4.2	0.0043	<a href="#">73338</a>	PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS
MEDIUM	5.0*	3.6	0.0977	<a href="#">74291</a>	PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities
MEDIUM	6.8*	5.9	0.0796	<a href="#">77402</a>	PHP 5.4.x < 5.4.32 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	0.0627	<a href="#">79246</a>	PHP 5.4.x < 5.4.35 'donote' DoS
MEDIUM	5.0*	-	-	<a href="#">46803</a>	PHP expose_php Information Disclosure

MEDIUM	4.3*	-	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	-	-	<a href="#">85582</a>	Web Application Potentially Vulnerable to Clickjacking
LOW	3.7	3.6	0.5961	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	-	<a href="#">34324</a>	FTP Supports Cleartext Authentication
LOW	2.1*	4.2	0.8808	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	<a href="#">76791</a>	PHP 5.4.x < 5.4.31 CLI Server 'header' DoS
LOW	2.6*	-	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	-	<a href="#">42057</a>	Web Server Allows Password Auto-Completion
LOW	2.6*	-	-	<a href="#">26194</a>	Web Server Transmits Cleartext Credentials
INFO	N/A	-	-	<a href="#">46180</a>	Additional DNS Hostnames
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="#">39519</a>	Backported Security Patch Detection (FTP)
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="#">84239</a>	Debugging Log Report
INFO	N/A	-	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	-	<a href="#">18638</a>	Drupal Software Detection
INFO	N/A	-	-	<a href="#">194915</a>	Eclipse Jetty Web Server Detection
INFO	N/A	-	-	<a href="#">19689</a>	Embedded Web Server Detection
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="#">49704</a>	External URLs

INFO	N/A	-	-	<a href="#">10092</a>	FTP Server Detection
INFO	N/A	-	-	<a href="#">69826</a>	HTTP Cookie 'secure' Property Transport Mismatch
INFO	N/A	-	-	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	-	<a href="#">12053</a>	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	<a href="#">42410</a>	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	-	<a href="#">10394</a>	Microsoft Windows SMB Log In Possible
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="#">50344</a>	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	-	<a href="#">50345</a>	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	-	<a href="#">10719</a>	MySQL Server Detection
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">10335</a>	Nessus TCP scanner
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="#">48243</a>	PHP Version Detection
INFO	N/A	-	-	<a href="#">66334</a>	Patch Report
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="#">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="#">121010</a>	TLS Version 1.1 Protocol 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="#">135860</a>	WMI Not Available
INFO	N/A	-	-	<a href="#">85601</a>	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	-	<a href="#">85602</a>	Web Application Cookies Not Marked Secure
INFO	N/A	-	-	<a href="#">91815</a>	Web Application Sitemap
INFO	N/A	-	-	<a href="#">20108</a>	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	<a href="#">11032</a>	Web Server Directory Enumeration

INFO	N/A	-	-	10662	Web mirroring
INFO	N/A	-	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	17219	phpMyAdmin Detection

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