tenable® Nessus

My Basic Network Scan

Vulnerabilities by Host

Vulnerabilities by Host

192.168.10.1

6	5	12	2	59
CRITICAL	HIGH	MEDIUM	LOW	INFO
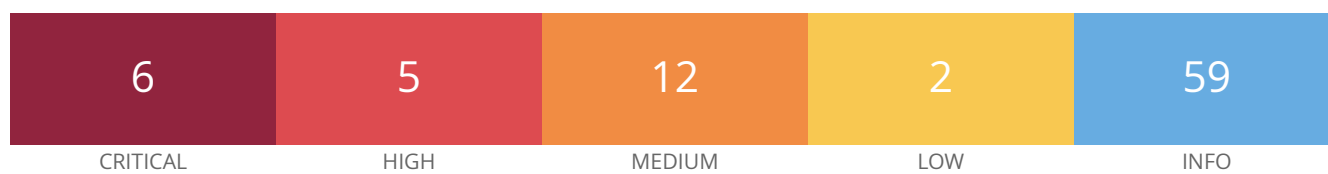
Vulnerabilities   Total: 84

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
CRITICAL	9.8	6.7	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CRITICAL	9.8	6.7	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
CRITICAL	9.8	6.7	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
CRITICAL	9.8	7.4	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
HIGH	8.8	5.9	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
HIGH	7.5	4.4	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
HIGH	7.5	8.4	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
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	6.1	3.6	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	6.1	3.8	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
MEDIUM	5.9	6.9	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.7	4.4	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
MEDIUM	5.0*	3.6	10073	Finger Recursive Request Arbitrary Site Redirection
LOW	3.7	1.4	38208	Apache Struts 2 s:a / s:url Tag href Element XSS
LOW	3.3*	-	10663	DHCP Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
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	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	43829	Kerberos Information Disclosure
INFO	N/A	-	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	-	20870	LDAP Server Detection
INFO	N/A	-	45478	LDAP User Enumeration
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	10185	POP Server Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	10263	SMTP Server Detection
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	-	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	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
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	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	33139	WS-Management Server Detection
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
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

192.168.10.2

0	**1**	**8**	**0**	**52**
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 61

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
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	5.9	6.9	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.3	2.2	10704	Apache Multiviews Arbitrary Directory Listing
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
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	-	43829	Kerberos Information Disclosure
INFO	N/A	-	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	-	20870	LDAP Server Detection
INFO	N/A	-	45478	LDAP User Enumeration
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
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	-	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	-	22964	Service Detection
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
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	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	33139	WS-Management Server 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