tenable® Nessus

ScanNessus_1_0

Report generated by Nessus™

Tue, 05 Sep 2023 09:00:42 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.1.1

1	2	8	1	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 38

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
HIGH	7.5	-	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	-	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	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	6.1	-	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
LOW	N/A	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
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	-	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	-	106658	JQuery Detection

INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
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	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information

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

192.168.1.3

0	1	2	0	16
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 19

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5*	-	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.0*	-	76474	SNMP 'GETBULK' Reflection DDoS
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	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	35296	SNMP Protocol Version Detection
INFO	N/A	-	34022	SNMP Query Routing Information Disclosure
INFO	N/A	-	10800	SNMP Query System Information Disclosure
INFO	N/A	-	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	40448	SNMP Supported Protocols Detection
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

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

192.168.1.5

1	3	2	0	30
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 36

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	56997	VMware ESX / ESXi Unsupported Version Detection
HIGH	8.8	-	168828	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0030)
HIGH	7.8	-	158494	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004)
HIGH	7.5	-	176249	ESXi < 7.0 Reflected Denial of Service
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
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	-	19689	Embedded Web Server Detection
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	-	10919	Open Port Re-check
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	175142	SLP Find Attributes
INFO	N/A	-	23777	SLP Server Detection (TCP)

INFO	N/A	-	23778	SLP Server Detection (UDP)
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	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20301	VMware ESX/GSX Server detection
INFO	N/A	-	57396	VMware vSphere Detect
INFO	N/A	-	10386	Web Server No 404 Error Code Check

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

192.168.1.11

0	0	0	0	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 26

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	-	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	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
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	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
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	-	100669	Web Application Cookies Are Expired

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

192.168.1.18

0	1	0	0	6
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5*	-	41028	SNMP Agent Default Community Name (public)
INFO	N/A	-	14274	Nessus SNMP Scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	40448	SNMP Supported Protocols Detection
INFO	N/A	-	10287	Traceroute Information
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

192.168.1.20

0	0	0	0	13
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 13

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	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	103869	Open Network Video Interface Forum (ONVIF) Protocol Detection
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

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

192.168.1.21

0	0	1	0	14
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.0*	-	12218	mDNS Detection (Remote Network)
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	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	103869	Open Network Video Interface Forum (ONVIF) Protocol Detection
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

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

192.168.1.22

0	0	1	0	14
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.0*	-	12218	mDNS Detection (Remote Network)
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	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	103869	Open Network Video Interface Forum (ONVIF) Protocol Detection
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

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

192.168.1.23

0	0	1	0	14
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.0*	-	12218	mDNS Detection (Remote Network)
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	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	103869	Open Network Video Interface Forum (ONVIF) Protocol Detection
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

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

192.168.1.24

0	0	1	0	14
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.0*	-	12218	mDNS Detection (Remote Network)
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	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	103869	Open Network Video Interface Forum (ONVIF) Protocol Detection
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

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

192.168.1.25

0	0	1	0	14
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.0*	-	12218	mDNS Detection (Remote Network)
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	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	103869	Open Network Video Interface Forum (ONVIF) Protocol Detection
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

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

192.168.1.95

1	3	5	0	60
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 69

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.3	-	15984	NFS Share User Mountable
HIGH	7.5*	-	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0*	-	12218	mDNS Detection (Remote Network)
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	45380	AFP Server Share Enumeration (guest)
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	10666	Apple Filing Protocol Server Detection
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
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	-	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	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	85805	HTTP/2 Cleartext Detection
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
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	-	10437	NFS Share Export List
INFO	N/A	-	14274	Nessus SNMP Scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	42823	Non-compliant Strict Transport Security (STS)
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	-	155705	QNAP QTS/QES/QuTS hero - Web Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	35296	SNMP Protocol Version Detection
INFO	N/A	-	34022	SNMP Query Routing Information Disclosure

INFO	N/A	-	10550	SNMP Query Running Process List Disclosure
INFO	N/A	-	10800	SNMP Query System Information Disclosure
INFO	N/A	-	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	40448	SNMP Supported Protocols 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	-	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	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
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	-	135860	WMI Not Available
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure

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

acceso.nextvision.lan

0	2	7	1	37
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 47

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	-	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	-	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	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3*	-	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	-	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
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	-	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	-	50845	OpenSSL Detection
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	10762	RTSP Server Type / Version Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
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	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	35297	SSL Service Requests Client Certificate
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	91263	SSL/TLS Service Requires Client Certificate
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
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	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

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

nvarbapp02.nextvision.lan

0	1	7	0	47
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 55

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	-	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	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.0	-	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
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	-	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	-	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	-	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	-	10180	Ping the remote host
INFO	N/A	-	66173	RDP Screenshot
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
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	-	35297	SSL Service Requests Client Certificate
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	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	135860	WMI Not Available
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