vulnerability scans

Report generated by Nessus™ Fri, 22 Apr 2022 14:50:00 MDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.8.....4
- 10.0.2.10.....7

Vulnerabilities by Host

10.0.2.8

Vulnerabilities Total: 53

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	8.8	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	9.3*	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	4.0	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only

MEDIUM	5.1*	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
MEDIUM	4.3*	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6*	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	14788	IP Protocols Scan
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	11936	OS Identification
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	66334	Patch Report
INFO	N/A	66173	RDP Screenshot

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	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	25220	TCP/IP Timestamps Supported
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	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled

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

10.0.2.10

Vulnerabilities Total: 69

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	123502	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : Firefox regression (USN-3918-3)
CRITICAL	9.8	124114	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : Firefox regressions (USN-3918-4)
CRITICAL	9.8	124085	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : Libxslt vulnerability (USN-3947-1)
CRITICAL	9.8	123751	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : busybox vulnerabilities (USN-3935-1)
CRITICAL	9.8	123973	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : wget vulnerabilities (USN-3943-1)
CRITICAL	9.8	159882	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : klibc vulnerabilities (USN-5379-1)
CRITICAL	9.8	123127	Ubuntu 14.04 LTS : Firefox vulnerabilities (USN-3918-2)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
HIGH	8.8	122811	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : LibTIFF vulnerabilities (USN-3906-1)
HIGH	8.1	123999	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : wpa_supplicant and hostapd vulnerabilities (USN-3944-1)
HIGH	8.1	125768	Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-4008-3)
HIGH	7.8	159982	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : Bash vulnerability (USN-5380-1)
HIGH	7.8	159160	Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel vulnerabilities (USN-5343-1)

HIGH	7.5	159255	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-5342-1)
HIGH	7.5	159725	Ubuntu 14.04 LTS / 16.04 LTS : Gzip vulnerability (USN-5378-4)
HIGH	7.5	159719	Ubuntu 14.04 LTS / 16.04 LTS : XZ Utils vulnerability (USN-5378-3)
HIGH	7.5	159361	Ubuntu 14.04 LTS / 16.04 LTS : zlib vulnerability (USN-5355-2)
HIGH	7.0	123930	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : systemd vulnerability (USN-3938-1)
MEDIUM	6.7	123750	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : policykit-1 vulnerability (USN-3934-1)
MEDIUM	6.7	122893	Ubuntu 14.04 LTS : Linux kernel (Xenial HWE) vulnerabilities (USN-3910-2)
MEDIUM	6.7	123681	Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3932-2)
MEDIUM	6.5	125144	Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3982-2) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)
MEDIUM	5.9	124759	Ubuntu 14.04 LTS : wpa vulnerability (USN-3969-2)
MEDIUM	5.5	123075	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : Ghostscript vulnerabilities (USN-3915-1)
MEDIUM	5.4	123931	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : samba vulnerability (USN-3939-1)
MEDIUM	4.3*	90317	SSH Weak Algorithms Supported
LOW	3.7	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	34098	BIOS Info (SSH)
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	132634	Deprecated SSLv2 Connection Attempts
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	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	14788	IP Protocols Scan
INFO	N/A	118237	JAR File Detection for Linux/UNIX
INFO	N/A	151883	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	95928	Linux User List Enumeration
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	64582	Netstat Connection Information
INFO	N/A	14272	Netstat Portscanner (SSH)
INFO	N/A	11936	OS Identification
INFO	N/A	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	117887	OS Security Patch Assessment Available
INFO	N/A	66334	Patch Report
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	102094	SSH Commands Require Privilege Escalation
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	90707	SSH SCP Protocol Detection
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection

INFO	N/A	22869	Software Enumeration (SSH)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110385	Target Credential Issues by Authentication Protocol - Insufficient Privilege
INFO	N/A	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	56468	Time of Last System Startup
INFO	N/A	10287	Traceroute Information
INFO	N/A	110483	Unix / Linux Running Processes Information
INFO	N/A	152742	Unix Software Discovery Commands Available
INFO	N/A	66717	mDNS Detection (Local Network)

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