nessus

Report generated by Nessus™

Ubuntu-16.04-No-ESM

Sun, 13 Feb 2022 21:00:47 PST

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.1.26

CRITICAL	HIGH	MEDIUM	LOW	INFO
13	21	14	0	76

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.9	157360	Samba 4.13.x < 4.13.17 / 4.14.x < 4.14.12 / 4.15.x < 4.15.5 Muiltiple Vulnerabilities
CRITICAL	9.8	154259	MySQL 5.7.x < 5.7.36 Multiple Vulnerabilities (Oct 2021 CPU)
CRITICAL	9.8	150394	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 / 21.04 : Intel Microcode vulnerabilities (USN-4985-1)
CRITICAL	9.8	156040	Ubuntu 16.04 LTS / 18.04 LTS : GLib vulnerability (USN-5189-1)
CRITICAL	9.8	157160	Ubuntu 16.04 LTS / 18.04 LTS : shadow vulnerabilities (USN-5254-1)
CRITICAL	9.8	150942	Ubuntu 16.04 LTS : Apache HTTP Server vulnerabilities (USN-4994-2)
CRITICAL	9.8	153766	Ubuntu 16.04 LTS : Apache HTTP Server vulnerabilities (USN-5090-2)
CRITICAL	9.8	156568	Ubuntu 16.04 LTS : Apache HTTP Server vulnerabilities (USN-5212-2)
CRITICAL	9.8	150712	Ubuntu 16.04 LTS : LZ4 vulnerability (USN-4968-2)
CRITICAL	9.8	157357	Ubuntu 16.04 LTS : Samba vulnerability (USN-5260-3)
CRITICAL	9.8	149905	Ubuntu 16.04 LTS : libx11 vulnerability (USN-4966-2)
CRITICAL	9.1	153448	Ubuntu 16.04 LTS : Python vulnerabilities (USN-5083-1)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
HIGH	8.8	153134	Ubuntu 16.04 LTS : Linux kernel vulnerability (USN-5062-1)
HIGH	8.6	150858	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 / 21.04 : libxml2 vulnerabilities (USN-4991-1)

HIGH	8.1	151969	MySQL 5.7.x < 5.7.35 Multiple Vulnerabilities (Jul 2021 CPU)
HIGH	8.1	153408	Ubuntu 16.04 LTS : Squashfs-Tools vulnerabilities (USN-5078-2)
HIGH	7.8	155351	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Vim vulnerabilities (USN-5147-1)
HIGH	7.8	153130	Ubuntu 16.04 LTS / 18.04 LTS / 21.04 : Linux kernel vulnerability (USN-5014-1)
HIGH	7.8	156914	Ubuntu 16.04 LTS : DBus vulnerability (USN-5244-1)
HIGH	7.8	157224	Ubuntu 16.04 LTS : GNU cpio vulnerability (USN-5064-2)
HIGH	7.8	152536	Ubuntu 16.04 LTS : Linux kernel vulnerability (USN-5039-1)
HIGH	7.8	157085	Ubuntu 16.04 LTS : PolicyKit vulnerability (USN-5252-2)
HIGH	7.5	153243	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Git vulnerability (USN-5076-1)
HIGH	7.5	156804	Ubuntu 16.04 LTS : Byobu vulnerability (USN-5234-1)
HIGH	7.5	153514	Ubuntu 16.04 LTS : Libgcrypt vulnerabilities (USN-5080-2)
HIGH	7.5	153406	Ubuntu 16.04 LTS : curl vulnerabilities (USN-5079-2)
HIGH	7.4	150028	Ubuntu 16.04 LTS : DHCP vulnerability (USN-4969-2)
HIGH	7.4	152868	Ubuntu 16.04 LTS : OpenSSL vulnerability (USN-5051-2)
HIGH	7.3	153779	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 21.04 : Vim vulnerabilities (USN-5093-1)
HIGH	7.1	152918	Ubuntu 16.04 LTS / 21.04 : APR vulnerability (USN-5056-1)
HIGH	7.1	149908	Ubuntu 16.04 LTS : Apport vulnerabilities (USN-4965-2)
HIGH	7.0	154569	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 21.04 / 21.10 : PHP vulnerability (USN-5125-1)
HIGH	7.0	156483	Ubuntu 16.04 LTS : Linux kernel vulnerability (USN-5211-1)
MEDIUM	6.7	157299	Ubuntu 16.04 LTS : Cron vulnerabilities (USN-5259-1)
MEDIUM	5.5	154903	Ubuntu 16.04 LTS / 18.04 LTS : ICU vulnerability (USN-5133-1)
MEDIUM	5.5	153366	Ubuntu 16.04 LTS : Apport vulnerabilities (USN-5077-2)
MEDIUM	5.5	151451	Ubuntu 16.04 LTS : Avahi vulnerability (USN-5008-2)
MEDIUM	5.5	154415	Ubuntu 16.04 LTS : MySQL vulnerabilities (USN-5123-2)
MEDIUM	5.5	157370	Ubuntu 16.04 LTS : MySQL vulnerabilities (USN-5270-2)
MEDIUM	5.5	151835	Ubuntu 16.04 LTS : systemd vulnerabilities (USN-5013-2)
MEDIUM	5.3	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	154709	Ubuntu 16.04 LTS : Bind vulnerability (USN-5126-2)
MEDIUM	5.3	151583	Ubuntu 16.04 LTS : PHP vulnerabilities (USN-5006-2)
MEDIUM	5.3	156918	Ubuntu 16.04 LTS : curl vulnerability (USN-5021-2)
MEDIUM	5.0	153942	Ubuntu 16.04 LTS : MySQL vulnerabilities (USN-5022-3)

MEDIUM	4.9	148936	MySQL 5.7.x < 5.7.34 Multiple Vulnerabilities (Apr 2021 CPU)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	142640	Apache HTTP Server Site Enumeration
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	156000	Apache Log4j Installed (Linux / Unix)
INFO	N/A	34098	BIOS Info (SSH)
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	35373	DNS Server DNSSEC Aware Resolver
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
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	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	11414	IMAP Service Banner Retrieval
INFO	N/A	151883	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	95928	Linux User List Enumeration
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
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	129468	MySQL Server Installed (Linux)
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	10185	POP Server Detection
INFO	N/A	66334	Patch Report
INFO	N/A	130024	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	102095	SSH Commands Ran With 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	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	22869	Software Enumeration (SSH)
INFO	N/A	35351	System Information Enumeration (via DMI)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110095	Target Credential Issues by Authentication Protocol - No Issues Found

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	153569	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 21.04 : Linux kernel vulnerability (USN-5086-1)
INFO	N/A	153781	Ubuntu 16.04 LTS : Apache HTTP Server regression (USN-5090-4)
INFO	N/A	154431	Ubuntu 16.04 LTS : Apport vulnerability (USN-5122-2)
INFO	N/A	152957	Ubuntu 16.04 LTS : NTFS-3G vulnerabilities (USN-5060-2)
INFO	N/A	153592	Ubuntu 16.04 LTS : ca-certificates update (USN-5089-2)
INFO	N/A	153510	Ubuntu 16.04 LTS : curl regression (USN-5079-4)
INFO	N/A	83303	Unix / Linux - Local Users Information : Passwords Never Expire
INFO	N/A	110483	Unix / Linux Running Processes Information
INFO	N/A	152743	Unix Software Discovery Commands Not Available
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

Hide