

Ubuntu-14.04-ESM

Mon, 14 Feb 2022 21:38:22 PST

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.1.30

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

192.168.1.30

2

CRITICAL

2

HIGH

9

MEDIUM

3

LOW

87

INFO

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 Multiple Vulnerabilities
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	20007	SSL Version 2 and 3 Protocol Detection
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	12085	Apache Tomcat Default Files
MEDIUM	5.3	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	4.9	138561	MySQL Denial of Service (Jul 2020 CPU)
MEDIUM	4.3*	90317	SSH Weak Algorithms Supported
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
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	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	39446	Apache Tomcat Detection
INFO	N/A	130175	Apache Tomcat Local Detection
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	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	42085	IMAP Service STARTTLS Command Support
INFO	N/A	147817	Java Detection and Identification (Linux / Unix)
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	148373	OpenJDK Java Detection (Linux / Unix)
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	10185	POP Server Detection
INFO	N/A	42087	POP3 Service STLS Command Support
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	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	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	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
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	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
INFO	N/A	66717	mDNS Detection (Local Network)

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

Hide