



# Windows Machine

Report generated by Nessus™

Thu, 11 Jan 2024 03:15:24 EST

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 10.0.2.15.....	4
------------------	---

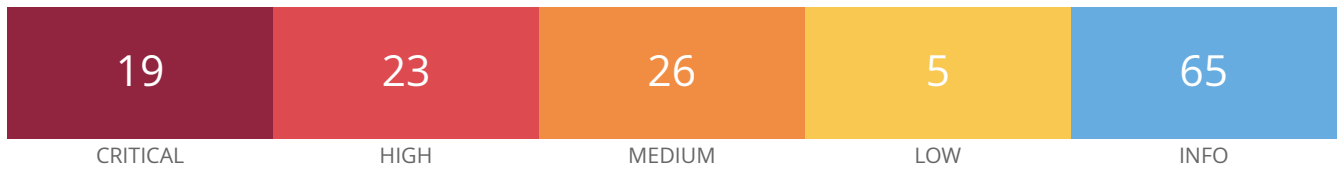
For Trial Use Only

---

## **Vulnerabilities by Host**

---

## 10.0.2.15



### Vulnerabilities

Total: 138

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	<a href="#">100995</a>	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	6.7	<a href="#">101787</a>	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	7.4	<a href="#">158900</a>	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	6.7	<a href="#">161948</a>	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	8.4	<a href="#">172186</a>	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	<a href="#">153584</a>	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	7.4	<a href="#">95438</a>	Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities
CRITICAL	9.8	6.7	<a href="#">111067</a>	Apache Tomcat 8.0.0 < 8.0.53 Security Constraint Weakness
CRITICAL	9.8	9.0	<a href="#">134862</a>	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	9.7	<a href="#">125313</a>	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	9.1	6.0	<a href="#">121120</a>	Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control
CRITICAL	9.0	6.5	<a href="#">170113</a>	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	<a href="#">153583</a>	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	<a href="#">171342</a>	Apache Tomcat SEoL (8.0.x)
CRITICAL	10.0	-	<a href="#">171356</a>	Apache httpd SEoL (2.1.x <= x <= 2.2.x)
CRITICAL	10.0	-	<a href="#">58987</a>	PHP Unsupported Version Detection
CRITICAL	10.0	-	<a href="#">108797</a>	Unsupported Windows OS (remote)

CRITICAL	10.0*	7.3	<a href="#">53514</a>	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0*	5.9	<a href="#">60085</a>	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	8.1	9.2	<a href="#">103697</a>	Apache Tomcat 8.0.0.RC1 < 8.0.47 Multiple Vulnerabilities
HIGH	8.1	9.7	<a href="#">97833</a>	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)
HIGH	7.5	4.4	<a href="#">183391</a>	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	4.4	<a href="#">96003</a>	Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure
HIGH	7.5	6.0	<a href="#">94578</a>	Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities
HIGH	7.5	4.4	<a href="#">99367</a>	Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure
HIGH	7.5	4.4	<a href="#">121119</a>	Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service
HIGH	7.5	4.4	<a href="#">100681</a>	Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation
HIGH	7.5	3.6	<a href="#">121124</a>	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service
HIGH	7.5	-	<a href="#">142591</a>	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	4.9	<a href="#">35291</a>	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	6.1	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	7.4	<a href="#">77531</a>	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
HIGH	7.3	5.9	<a href="#">66584</a>	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities
HIGH	7.3	6.7	<a href="#">71426</a>	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities
HIGH	7.3	5.9	<a href="#">77285</a>	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.0	5.9	<a href="#">62101</a>	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities

HIGH	9.3*	9.6	<a href="#">58435</a>	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	7.5*	7.4	<a href="#">59056</a>	PHP 5.3.x < 5.3.13 CGI Query String Code Execution
HIGH	7.5*	6.7	<a href="#">59529</a>	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities
HIGH	7.5*	5.9	<a href="#">64992</a>	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities
HIGH	7.5*	8.9	<a href="#">58988</a>	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	5.2	<a href="#">41028</a>	SNMP Agent Default Community Name (public)
MEDIUM	6.8	6.0	<a href="#">90510</a>	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	2.5	<a href="#">18405</a>	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.5	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	<a href="#">157288</a>	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	7.1	<a href="#">187315</a>	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.9	4.4	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.6	3.4	<a href="#">68915</a>	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.3	7.3	<a href="#">57791</a>	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.3	3.0	<a href="#">64912</a>	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	5.3	1.4	<a href="#">73405</a>	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.3	-	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	4.0	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	2.2	<a href="#">10546</a>	Microsoft Windows LAN Manager SNMP LanMan Users Disclosure
MEDIUM	5.3	-	<a href="#">152853</a>	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	<a href="#">15901</a>	SSL Certificate Expiry

MEDIUM	5.3	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	4.3	2.2	<a href="#">102588</a>	Apache Tomcat 8.0.0.RC1 < 8.0.45 Cache Poisoning
MEDIUM	4.0	-	<a href="#">58453</a>	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	5.0*	3.6	<a href="#">66842</a>	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities
MEDIUM	6.8*	5.9	<a href="#">67259</a>	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	<a href="#">58966</a>	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	<a href="#">73289</a>	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	4.3*	-	<a href="#">57690</a>	Terminal Services Encryption Level is Medium or Low
LOW	3.7	4.4	<a href="#">106976</a>	Apache Tomcat 8.0.0.RC1 < 8.0.50 Security Constraint Weakness
LOW	3.7	2.2	<a href="#">159462</a>	Apache Tomcat 8.x < 8.5.78 Spring4Shell (CVE-2022-22965) Mitigations
LOW	3.7	4.5	<a href="#">83875</a>	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	N/A	2.2	<a href="#">10547</a>	Microsoft Windows LAN Manager SNMP LanMan Services Disclosure
LOW	2.6*	-	<a href="#">30218</a>	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	-	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	<a href="#">21186</a>	AJP Connector Detection
INFO	N/A	-	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	-	<a href="#">39446</a>	Apache Tomcat Detection
INFO	N/A	-	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	<a href="#">10736</a>	DCE Services Enumeration
INFO	N/A	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	-	<a href="#">10107</a>	HTTP Server Type and Version

INFO	N/A	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	<a href="#">53513</a>	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	<a href="#">26917</a>	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	<a href="#">14274</a>	Nessus SNMP Scanner
INFO	N/A	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	<a href="#">24786</a>	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	<a href="#">181418</a>	OpenSSH Detection
INFO	N/A	-	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	-	<a href="#">48243</a>	PHP Version Detection
INFO	N/A	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	<a href="#">66173</a>	RDP Screenshot
INFO	N/A	-	<a href="#">10940</a>	Remote Desktop Protocol Service Detection
INFO	N/A	-	<a href="#">35296</a>	SNMP Protocol Version Detection
INFO	N/A	-	<a href="#">19763</a>	SNMP Query Installed Software Disclosure
INFO	N/A	-	<a href="#">34022</a>	SNMP Query Routing Information Disclosure
INFO	N/A	-	<a href="#">10550</a>	SNMP Query Running Process List Disclosure
INFO	N/A	-	<a href="#">10800</a>	SNMP Query System Information Disclosure
INFO	N/A	-	<a href="#">10551</a>	SNMP Request Network Interfaces Enumeration



INFO	N/A	-	<a href="#">185519</a>	SNMP Server Detection
INFO	N/A	-	<a href="#">40448</a>	SNMP Supported Protocols Detection
INFO	N/A	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	<a href="#">45410</a>	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	<a href="#">94761</a>	SSL Root Certification Authority Certificate Information
INFO	N/A	-	<a href="#">51891</a>	SSL Session Resume Supported
INFO	N/A	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	<a href="#">17975</a>	Service Detection (GET request)
INFO	N/A	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	<a href="#">121010</a>	TLS Version 1.1 Protocol Detection
INFO	N/A	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	<a href="#">64814</a>	Terminal Services Use SSL/TLS

INFO	N/A	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	<a href="#">20108</a>	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	<a href="#">11422</a>	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	<a href="#">11424</a>	WebDAV Detection
INFO	N/A	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure

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