tenable® Nessus

Mr.Blue2

Report generated by Tenable Nessus™ Sat, 09 Nov 2024 03:06:08 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.10.59.100

2	2	5	2	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 32

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentiale check)
CRITICAL	10.0	-	-	108797	Unsupported Windows OS (remote)
HIGH	8.1	-	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3*	9.6	0.7644	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Rem Code Execution (2671387) (uncredentialed check)
MEDIUM	6.8	-	-	90510	MS16-047: Security Update for SAM and LSAD Remote Protoco (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	2.5	0.0127	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	4.0	-	-	58453	Terminal Services Doesn't Use Network Level Authentication (Only
MEDIUM	4.3*	-	-	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	86420	Ethernet MAC Addresses

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 (remo 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	-	-	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	-	-	10287	Traceroute Information
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