Nessus Scan Report

27/Jun/2013:05:12:40

Table Of Contents

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

192.168.1.146

Summary

Critical	High	Medium	Low	Info	Total
17	2	10	2	47	78

Details

Severity	Plugin Id	Name
Critical (10.0)	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)
Critical (10.0)	11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
Critical (10.0)	11890	MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check)
Critical (10.0)	12054	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM)

Critical (10.0)	12209	MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)
Critical (10.0)	13852	MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) (uncredentialed check)
Critical (10.0)	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
Critical (10.0)	19407	MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)
Critical (10.0)	19408	MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)
Critical (10.0)	20008	MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution (902400) (uncredentialed check)
Critical (10.0)	21193	MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)
Critical (10.0)	21334	MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow DoS (913580) (uncredentialed check)
Critical (10.0)	21655	MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncredentialed check)
Critical (10.0)	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
Critical (10.0)	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)
Critical (10.0)	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
Critical (10.0)	47709	Microsoft Windows 2000 Unsupported Installation Detection
High (7.5)	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
High (7.5)	34460	Unsupported Web Server Detection
Medium (5.0)	10079	Anonymous FTP Enabled
Medium (5.0)	10956	Microsoft IIS / Site Server codebrws.asp Arbitrary Source Disclosure
Medium (5.0)	18585	Microsoft Windows SMB Service Enumeration via \srvsvc
Medium (5.0)	18602	Microsoft Windows SMB svcctl MSRPC Interface SCM Service Enumeration
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication

Medium (5.0)	45517	MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)
Medium (5.0)	56210	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials
Medium (5.0)	56211	SMB Use Host SID to Enumerate Local Users Without Credentials
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Low (3.3)	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
Low (2.6)	34324	FTP Supports Clear Text Authentication
Info	10077	Microsoft FrontPage Extensions Check
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10263	SMTP Server Detection
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10661	Microsoft IIS 5 .printer ISAPI Filter Enabled
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10904	Microsoft Windows 'Backup Operators' Group User List

Info	10913	Microsoft Windows - Local Users Information : Disabled accounts
Info	10914	Microsoft Windows - Local Users Information : Never changed passwords
Info	10915	Microsoft Windows - Local Users Information : User has never logged on
Info	10916	Microsoft Windows - Local Users Information : Passwords never expire
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11422	Web Server Unconfigured - Default Install Page Present
Info	11424	WebDAV Detection
Info	11874	Microsoft IIS 404 Response Service Pack Signature
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	17975	Service Detection (GET request)
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21745	Authentication Failure - Local Checks Not Run
Info	22319	MSRPC Service Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24269	Windows Management Instrumentation (WMI) Available
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35705	SMB Registry : Starting the Registry Service during the scan failed
Info	35716	Ethernet Card Manufacturer Detection

Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	59861	Remote web server screenshot
Info	66334	Patch Report