Windows hack

Report generated by Nessus™ Sun, 10 Mar 2019 13:46:33 CST

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary

192.168.0.252

Vulnerabilities Total: 131

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	57603	Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow
CRITICAL	10.0	45004	Apache 2.2.x < 2.2.15 Multiple Vulnerabilities
CRITICAL	10.0	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (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) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	10.0	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	78555	OpenSSL Unsupported
CRITICAL	10.0	55925	PHP 5.3 < 5.3.7 Multiple Vulnerabilities
CRITICAL	10.0	60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	9.3	74363	OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities
HIGH	9.3	57459	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	9.3	48245	PHP 5.3 < 5.3.3 Multiple Vulnerabilities

HIGH	8.5	59529	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities
HIGH	7.6	17766	OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow
HIGH	7.5	42052	Apache 2.2.x < 2.2.14 Multiple Vulnerabilities
HIGH	7.5	77531	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
HIGH	7.5	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
HIGH	7.5	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
HIGH	7.5	10081	FTP Privileged Port Bounce Scan
HIGH	7.5	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
HIGH	7.5	58799	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
HIGH	7.5	52717	PHP 5.3 < 5.3.6 Multiple Vulnerabilities
HIGH	7.5	59056	PHP 5.3.x < 5.3.13 CGI Query String Code Execution
HIGH	7.5	64992	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities
HIGH	7.5	66584	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities
HIGH	7.5	71426	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities
HIGH	7.5	77285	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.5	58966	PHP < 5.3.11 Multiple Vulnerabilities
HIGH	7.5	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5	57537	PHP < 5.3.9 Multiple Vulnerabilities
HIGH	7.5	34460	Unsupported Web Server Detection
HIGH	7.1	77086	OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.9	62101	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities
MEDIUM	6.8	82030	OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities
MEDIUM	6.8	84151	OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities
MEDIUM	6.8	42862	PHP 5.3 < 5.3.1 Multiple Vulnerabilities

MEDIUM	6.8	51140	PHP 5.3 < 5.3.4 Multiple Vulnerabilities
MEDIUM	6.8	67259	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities
MEDIUM	6.4	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.1	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.1	17765	OpenSSL < 0.9.8l Multiple Vulnerabilities
MEDIUM	5.0	48205	Apache 2.2.x < 2.2.16 Multiple Vulnerabilities
MEDIUM	5.0	50070	Apache 2.2.x < 2.2.17 Multiple Vulnerabilities
MEDIUM	5.0	57791	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.0	73405	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.0	10678	Apache mod_info /server-info Information Disclosure
MEDIUM	5.0	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.0	59076	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service
MEDIUM	5.0	80566	OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)
MEDIUM	5.0	87219	OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS
MEDIUM	5.0	58564	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	5.0	51439	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS
MEDIUM	5.0	66842	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities
MEDIUM	5.0	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname

MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	53896	Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS
MEDIUM	4.3	56216	Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS
MEDIUM	4.3	64912	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	4.3	78552	OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)
MEDIUM	4.3	17767	OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability
MEDIUM	4.3	64532	OpenSSL < 0.9.8y Multiple Vulnerabilities
MEDIUM	4.3	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	10107	HTTP Server Type and Version

INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
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 Dialects Supported (remote check)
INFO	N/A	10719	MySQL Server Detection
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	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	56984	SSL / TLS Versions Supported

INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	42981	SSL Certificate Expiry - Future Expiry
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	62563	SSL Compression Methods Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	11424	WebDAV Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure