BAD STORE

Vulnerabilities by Host

Vulnerabilities by Host

192.168.152.135

7	**6**	**17**	**2**	**17**
CRITICAL	HIGH	MEDIUM	LOW	INFO
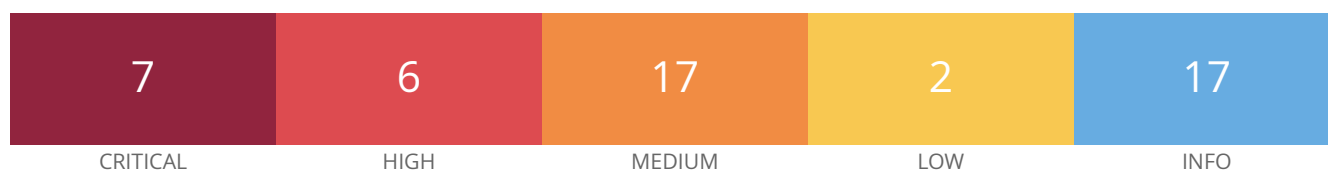
Vulnerabilities   Total: 49

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	11915	Apache < 1.3.29 Multiple Modules Local Overflow
CRITICAL	9.8	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.0	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	78555	OpenSSL Unsupported
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0*	15555	Apache mod_proxy Content-Length Overflow
CRITICAL	10.0*	17757	OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities
HIGH	7.3	31654	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow
HIGH	7.5*	13651	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String
HIGH	9.3*	17760	OpenSSL < 0.9.8f Multiple Vulnerabilities
HIGH	9.3*	57459	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	7.5*	58799	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
HIGH	7.5*	12255	mod_ssl ssl_util_uuencode_binary Remote Overflow
MEDIUM	6.5	17696	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM	5.3	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	40984	Browsable Web Directories
MEDIUM	5.3	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0*	59076	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service

MEDIUM	5.0*	17750	OpenSSL < 0.9.6m / 0.9.7d Denial of Service
MEDIUM	5.0*	12110	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS
MEDIUM	5.0*	17755	OpenSSL < 0.9.7h / 0.9.8a Protocol Version Rollback
MEDIUM	4.3*	17756	OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability
MEDIUM	5.0*	17759	OpenSSL < 0.9.8 Weak Default Configuration
MEDIUM	4.3*	56996	OpenSSL < 0.9.8h Multiple Vulnerabilities
MEDIUM	5.0*	17761	OpenSSL < 0.9.8i Denial of Service
MEDIUM	5.8*	17762	OpenSSL < 0.9.8j Signature Spoofing
MEDIUM	5.0*	17763	OpenSSL < 0.9.8k Multiple Vulnerabilities
MEDIUM	5.1*	17765	OpenSSL < 0.9.8l Multiple Vulnerabilities
MEDIUM	5.0*	58564	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	4.3*	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	2.1*	17754	OpenSSL < 0.9.7f Insecure Temporary File Creation
LOW	2.6*	64532	OpenSSL < 0.9.8y Multiple Vulnerabilities
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	49704	External URLs
INFO	N/A	84502	HSTS Missing From HTTPS Server
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	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	11219	Nessus SYN scanner

INFO	N/A	19506	Nessus Scan Information
INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	91815	Web Application Sitemap
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	11419	Web Server Office File Inventory
INFO	N/A	10302	Web Server robots.txt Information Disclosure
INFO	N/A	10662	Web mirroring

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