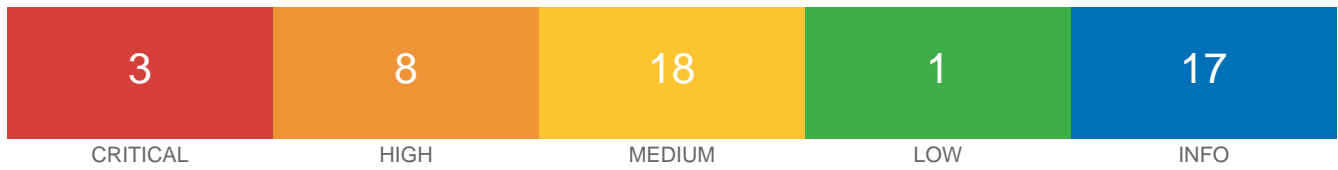


## 10.82.1.42



### Vulnerabilities

Total: 47

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	15555	Apache mod_proxy Content-Length Overflow
CRITICAL	10.0	17757	OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities
CRITICAL	10.0	78555	OpenSSL Unsupported
HIGH	9.3	17760	OpenSSL < 0.9.8f Multiple Vulnerabilities
HIGH	9.3	57459	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	7.5	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	7.5	58799	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
HIGH	7.5	34460	Unsupported Web Server Detection
HIGH	7.5	12255	mod_ssl ssl_util_uuencode_binary Remote Overflow
HIGH	7.2	11915	Apache < 1.3.29 Multiple Modules Local Overflow
MEDIUM	5.8	17762	OpenSSL < 0.9.8j Signature Spoofing
MEDIUM	5.1	17765	OpenSSL < 0.9.8l Multiple Vulnerabilities
MEDIUM	5.0	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.0	40984	Browsable Web Directories
MEDIUM	5.0	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	<a href="#">17755</a>	OpenSSL < 0.9.7h / 0.9.8a Protocol Version Rollback
MEDIUM	5.0	<a href="#">17759</a>	OpenSSL < 0.9.8 Weak Default Configuration
MEDIUM	5.0	<a href="#">17761</a>	OpenSSL < 0.9.8i Denial of Service
MEDIUM	5.0	<a href="#">17763</a>	OpenSSL < 0.9.8k Multiple Vulnerabilities
MEDIUM	5.0	<a href="#">58564</a>	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	4.3	<a href="#">17696</a>	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM	4.3	<a href="#">17756</a>	OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability
MEDIUM	4.3	<a href="#">56996</a>	OpenSSL < 0.9.8h Multiple Vulnerabilities
MEDIUM	4.3	<a href="#">64532</a>	OpenSSL < 0.9.8y Multiple Vulnerabilities
MEDIUM	4.3	<a href="#">85582</a>	Web Application Potentially Vulnerable to Clickjacking
LOW	2.1	<a href="#">17754</a>	OpenSSL < 0.9.7f Insecure Temporary File Creation
INFO	N/A	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	<a href="#">33817</a>	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	<a href="#">49704</a>	External URLs
INFO	N/A	<a href="#">84502</a>	HSTS Missing From HTTPS Server
INFO	N/A	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
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="#">50344</a>	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	<a href="#">50345</a>	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	<a href="#">57323</a>	OpenSSL Version Detection
INFO	N/A	<a href="#">91815</a>	Web Application Sitemap

---

INFO	N/A	<a href="#">11032</a>	Web Server Directory Enumeration
INFO	N/A	<a href="#">11419</a>	Web Server Office File Inventory
INFO	N/A	<a href="#">10302</a>	Web Server robots.txt Information Disclosure
INFO	N/A	<a href="#">10662</a>	Web mirroring

---