PaginaZero_PaolaJuan

Vulnerabilities by Host

Vulnerabilities by Host

zero.webappsecurity.com

5	17	66	3	33
CRITICAL	HIGH	MEDIUM	LOW	INFO
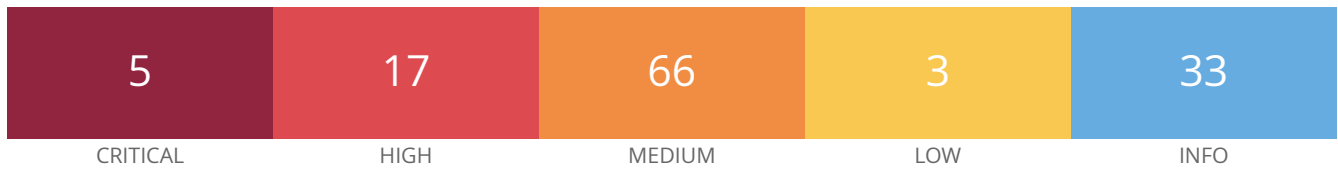
Vulnerabilities

Total: 124

SEVERITY	CVSS V2.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	6.7	57603	Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow
CRITICAL	10.0	9.0	45004	Apache 2.2.x < 2.2.15 Multiple Vulnerabilities
CRITICAL	10.0	9.0	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	10.0	-	78555	OpenSSL Unsupported
CRITICAL	10.0	-	20007	SSL Version 2 and 3 Protocol Detection
HIGH	9.3	5.9	17760	OpenSSL < 0.9.8f Multiple Vulnerabilities
HIGH	9.3	5.9	57459	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	7.8	6.4	40467	Apache 2.2.x < 2.2.12 Multiple Vulnerabilities
HIGH	7.6	7.3	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
HIGH	7.6	5.9	17766	OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow
HIGH	7.5	6.7	42052	Apache 2.2.x < 2.2.14 Multiple Vulnerabilities
HIGH	7.5	6.7	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
HIGH	7.5	6.7	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
HIGH	7.5	7.4	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
HIGH	7.5	7.4	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	7.4	153584	Apache < 2.4.49 Multiple Vulnerabilities
HIGH	7.5	5.9	95438	Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities
HIGH	7.5	6.7	111066	Apache Tomcat 7.0.41 < 7.0.90 Multiple Vulnerabilities

HIGH	7.5	8.9	133845	Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities
HIGH	7.5	-	171351	Apache Tomcat Web Server SEoL (7.0.x)
HIGH	7.5	-	171356	Apache httpd SEoL (2.1.x <= x <= 2.2.x)
HIGH	7.5	6.7	58799	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
MEDIUM	6.9	6.7	62101	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities
MEDIUM	6.8	8.4	77531	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
MEDIUM	6.8	8.1	153583	Apache < 2.4.49 Multiple Vulnerabilities
MEDIUM	6.8	8.9	103329	Apache Tomcat 7.0.x < 7.0.81 Multiple Vulnerabilities
MEDIUM	6.8	9.2	103698	Apache Tomcat 7.0.x < 7.0.82 / 8.5.x < 8.5.23 Multiple Vulnerabilities
MEDIUM	6.8	9.2	103782	Apache Tomcat 7.0.x < 7.0.82 Multiple Vulnerabilities
MEDIUM	6.8	8.3	74363	OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities
MEDIUM	6.8	5.9	82030	OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities
MEDIUM	6.8	5.9	84151	OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities
MEDIUM	6.4	5.2	121120	Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control
MEDIUM	6.4	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.1	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	5.0	151502	Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability
MEDIUM	5.8	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	5.8	4.0	17762	OpenSSL < 0.9.8j Signature Spoofing
MEDIUM	5.8	7.7	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
MEDIUM	5.1	4.2	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.1	6.7	17765	OpenSSL < 0.9.8l Multiple Vulnerabilities
MEDIUM	5.0	3.6	48205	Apache 2.2.x < 2.2.16 Multiple Vulnerabilities
MEDIUM	5.0	4.4	50070	Apache 2.2.x < 2.2.17 Multiple Vulnerabilities

MEDIUM	5.0	8.3	57791	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.0	1.4	73405	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.0	3.6	96003	Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure
MEDIUM	5.0	6.0	94578	Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities
MEDIUM	5.0	3.6	99367	Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure
MEDIUM	5.0	5.1	138851	Apache Tomcat 7.0.x < 7.0.105 WebSocket DoS
MEDIUM	5.0	4.4	100681	Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation
MEDIUM	5.0	3.6	121121	Apache Tomcat 7.0.x < 7.0.88 Denial of Service
MEDIUM	5.0	-	12085	Apache Tomcat Default Files
MEDIUM	5.0	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	4.2	10539	DNS Server Recursive Query Cache Poisoning Weakness
MEDIUM	5.0	3.6	35450	DNS Server Spoofed Request Amplification DDoS
MEDIUM	5.0	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	2.7	15753	Multiple Vendor DNS Response Flooding Denial Of Service
MEDIUM	5.0	5.9	59076	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service
MEDIUM	5.0	4.5	80566	OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)
MEDIUM	5.0	2.2	87219	OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS
MEDIUM	5.0	5.1	17761	OpenSSL < 0.9.8i Denial of Service
MEDIUM	5.0	3.6	17763	OpenSSL < 0.9.8k Multiple Vulnerabilities
MEDIUM	5.0	3.6	58564	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	5.0	-	15901	SSL Certificate Expiry
MEDIUM	5.0	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

MEDIUM	4.4	8.4	136770	Apache Tomcat 7.0.0 < 7.0.104 Remote Code Execution
MEDIUM	4.4	8.4	147163	Apache Tomcat 7.0.0 < 7.0.108 RCE
MEDIUM	4.3	2.2	53896	Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS
MEDIUM	4.3	2.2	56216	Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS
MEDIUM	4.3	3.0	64912	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	4.3	3.8	31118	Apache 2.2.x < 2.2.8 Multiple Vulnerabilities (XSS, DoS)
MEDIUM	4.3	4.4	33477	Apache 2.2.x < 2.2.9 Multiple Vulnerabilities (DoS, XSS)
MEDIUM	4.3	3.3	17696	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM	4.3	1.4	88098	Apache Server ETag Header Information Disclosure
MEDIUM	4.3	5.1	148405	Apache Tomcat 7.0.0 < 7.0.107 Information Disclosure
MEDIUM	4.3	4.4	106975	Apache Tomcat 7.0.0 < 7.0.85 Security Constraint Weakness
MEDIUM	4.3	2.2	118035	Apache Tomcat 7.0.0 < 7.0.91 Open Redirect Weakness
MEDIUM	4.3	1.4	102587	Apache Tomcat 7.0.41 < 7.0.79 Cache Poisoning Vulnerability
MEDIUM	4.3	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	4.3	3.6	77086	OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities
MEDIUM	4.3	5.3	78552	OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)
MEDIUM	4.3	4.2	56996	OpenSSL < 0.9.8h Multiple Vulnerabilities
MEDIUM	4.3	4.2	17767	OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability
MEDIUM	4.3	2.7	51892	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
MEDIUM	4.3	5.1	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	4.3	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

LOW	2.6	3.6	64532	OpenSSL < 0.9.8y Multiple Vulnerabilities
LOW	2.6	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.6	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	72779	DNS Server Version Detection
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
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	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	57323	OpenSSL Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

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	-	58768	SSL Resume With Different Cipher Issue
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information