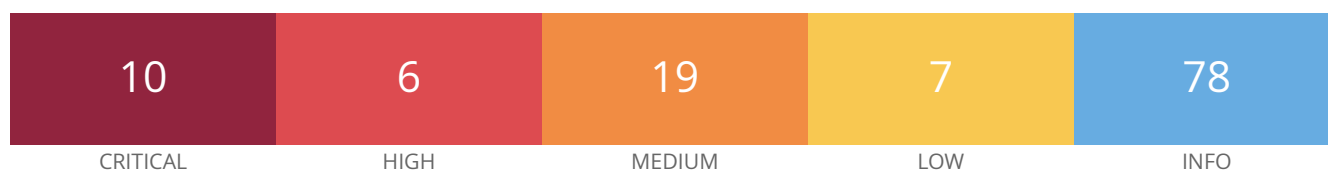


## 192.168.1.3



### Vulnerabilities

Total: 120

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.2	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	10205	rlogin Service Detection
HIGH	7.5*	6.7	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

MEDIUM	6.5	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	<a href="#">42263</a>	Unencrypted Telnet Server
MEDIUM	5.9	5.1	<a href="#">136808</a>	ISC BIND Denial of Service
MEDIUM	5.9	3.6	<a href="#">31705</a>	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	<a href="#">89058</a>	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	-	<a href="#">12217</a>	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	<a href="#">26928</a>	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	<a href="#">83875</a>	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.3	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	2.5	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	<a href="#">10407</a>	X Server Detection