Version 10.3.0-debian9_amd64

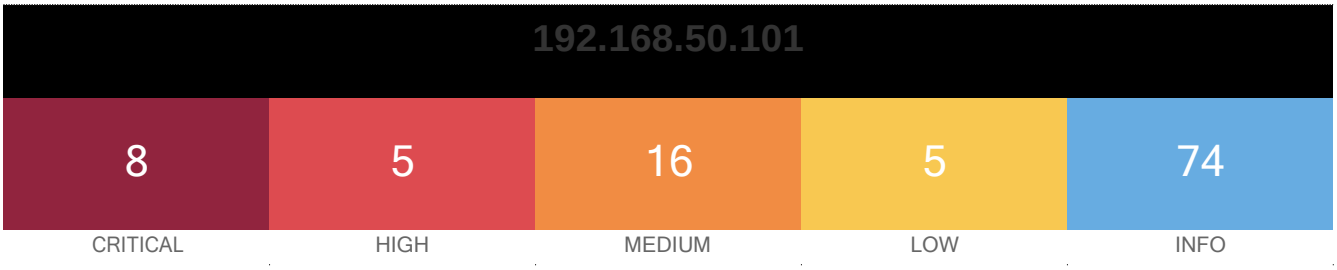
METASPLOITABLE

Report generated by Nessus™ Thu, 04 Aug 2022 09:03:51 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host



Vulnerabilities Total: 108

SEVERITY	CVSS V3.0	NAME
CRITICAL	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	Bind Shell Backdoor Detection
CRITICAL	9.8	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	NFS Exported Share Information Disclosure
CRITICAL	10.0*	VNC Server 'password' Password
HIGH	8.6	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	ISC BIND Denial of Service
HIGH	7.5	NFS Shares World Readable
HIGH	7.5	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	Samba Badlock Vulnerability
MEDIUM	6.8	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	SSL Self-Signed Certificate

MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	15901	SSL Certificate Expiry
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

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