REPORT META

REPORT META 24/01/2024

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

# Vulnerabilità

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Plugin ID** | **Name** | **Description** | **Risk** | **Solution** |
| 33850 | Unix Operating System Unsupported Version Detection | The operating system running on the remote host is no longer supported. | Critical | Moderata |
| 171340 | Apache Tomcat SEoL (<= 5.5.x) | An unsupported version of Apache Tomcat is installed on the remote host. | Critical | Moderata |
| 20007 | SSL Version 2 and 3 Protocol Detection | The remote service encrypts traffic using a protocol with known weaknesses. | Critical | Moderata |
| 20007 | SSL Version 2 and 3 Protocol Detection | The remote service encrypts traffic using a protocol with known weaknesses. | Critical | Moderata |
| 51988 | Bind Shell Backdoor Detection | The remote host may have been compromised. | Critical | Difficile |
| 11356 | NFS Exported Share Information Disclosure | It is possible to access NFS shares on the remote host. | Critical | Moderata |
| 11356 | NFS Exported Share Information Disclosure | It is possible to access NFS shares on the remote host. | Critical | Moderata |
| 11356 | NFS Exported Share Information Disclosure | It is possible to access NFS shares on the remote host. | Critical | Moderata |
| 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness | The remote SSH host keys are weak. | Critical | Difficile |
| 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) | The remote SSL certificate uses a weak key. | Critical | Difficile |
| 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) | The remote SSL certificate uses a weak key. | Critical | Difficile |
| 46882 | UnrealIRCd Backdoor Detection | The remote IRC server contains a backdoor. | Critical | Facile |
| 61708 | VNC Server 'password' Password | A VNC server running on the remote host is secured with a weak password. | Critical | Facile |
| 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | There is a vulnerable AJP connector listening on the remote host. | Critical | Moderata |
| 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | There is a vulnerable AJP connector listening on the remote host. | Critical | Moderata |
| 10205 | rlogin Service Detection | The rlogin service is running on the remote host. | High | Moderata |
| 10245 | rsh Service Detection | The rsh service is running on the remote host. | High | Moderata |
| 90509 | Samba Badlock Vulnerability | An SMB server running on the remote host is affected by the Badlock vulnerability. | High | Moderata |
| 136769 | ISC BIND Service Downgrade / Reflected DoS | The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities. | High | Moderata |
| 42256 | NFS Shares World Readable | The remote NFS server exports world-readable shares. | High | Moderata |
| 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) | The remote service supports the use of medium strength SSL ciphers. | High | Moderata |
| 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) | The remote service supports the use of medium strength SSL ciphers. | High | Moderata |
| 51192 | SSL Certificate Cannot Be Trusted | The SSL certificate for this service cannot be trusted. | Medium | Moderata |
| 51192 | SSL Certificate Cannot Be Trusted | The SSL certificate for this service cannot be trusted. | Medium | Moderata |
| 57582 | SSL Self-Signed Certificate | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. | Medium | Moderata |
| 57582 | SSL Self-Signed Certificate | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. | Medium | Moderata |
| 104743 | TLS Version 1.0 Protocol Detection | The remote service encrypts traffic using an older version of TLS. | Medium | Moderata |
| 104743 | TLS Version 1.0 Protocol Detection | The remote service encrypts traffic using an older version of TLS. | Medium | Moderata |
| 42263 | Unencrypted Telnet Server | The remote Telnet server transmits traffic in cleartext. | Medium | Moderata |
| 11213 | HTTP TRACE / TRACK Methods Allowed | Debugging functions are enabled on the remote web server. | Medium | Moderata |
| 11213 | HTTP TRACE / TRACK Methods Allowed | Debugging functions are enabled on the remote web server. | Medium | Moderata |
| 11213 | HTTP TRACE / TRACK Methods Allowed | Debugging functions are enabled on the remote web server. | Medium | Moderata |
| 12085 | Apache Tomcat Default Files | The remote web server contains default files. | Medium | Moderata |
| 15901 | SSL Certificate Expiry | The remote server's SSL certificate has already expired. | Medium | Moderata |
| 15901 | SSL Certificate Expiry | The remote server's SSL certificate has already expired. | Medium | Moderata |
| 45411 | SSL Certificate with Wrong Hostname | The SSL certificate for this service is for a different host. | Medium | Moderata |
| 45411 | SSL Certificate with Wrong Hostname | The SSL certificate for this service is for a different host. | Medium | Moderata |
| 57608 | SMB Signing not required | Signing is not required on the remote SMB server. | Medium | Moderata |
| 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | The remote service supports the use of the RC4 cipher. | Medium | Moderata |
| 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | The remote service supports the use of the RC4 cipher. | Medium | Moderata |
| 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | The remote service supports the use of the RC4 cipher. | Medium | Moderata |
| 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | The remote service supports the use of the RC4 cipher. | Medium | Moderata |
| 89058 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) | The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic. | Medium | Moderata |
| 136808 | ISC BIND Denial of Service | The remote name server is affected by an assertion failure vulnerability. | Medium | Moderata |
| 26928 | SSL Weak Cipher Suites Supported | The remote service supports the use of weak SSL ciphers. | Medium | Moderata |
| 81606 | SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK) | The remote host supports a set of weak ciphers. | Medium | Moderata |
| 90317 | SSH Weak Algorithms Supported | The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all. | Medium | Moderata |
| 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS | The remote name server is affected by a denial of service vulnerability. | Medium | Moderata |
| 52611 | SMTP Service STARTTLS Plaintext Command Injection | The remote mail service allows plaintext command injection while  negotiating an encrypted communications channel. | Medium | Moderata |
| 52611 | SMTP Service STARTTLS Plaintext Command Injection | The remote mail service allows plaintext command injection while  negotiating an encrypted communications channel. | Medium | Moderata |
| 52611 | SMTP Service STARTTLS Plaintext Command Injection | The remote mail service allows plaintext command injection while  negotiating an encrypted communications channel. | Medium | Moderata |
| 52611 | SMTP Service STARTTLS Plaintext Command Injection | The remote mail service allows plaintext command injection while  negotiating an encrypted communications channel. | Medium | Moderata |
| 52611 | SMTP Service STARTTLS Plaintext Command Injection | The remote mail service allows plaintext command injection while  negotiating an encrypted communications channel. | Medium | Moderata |
| 52611 | SMTP Service STARTTLS Plaintext Command Injection | The remote mail service allows plaintext command injection while  negotiating an encrypted communications channel. | Medium | Moderata |
| 31705 | SSL Anonymous Cipher Suites Supported | The remote service supports the use of anonymous SSL ciphers. | Medium | Moderata |
| 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) | It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services. | Low | Moderata |
| 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) | It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services. | Low | Moderata |
| 70658 | SSH Server CBC Mode Ciphers Enabled | The SSH server is configured to use Cipher Block Chaining. | Low | Moderata |
| 83738 | SSL/TLS EXPORT\_DHE <= 512-bit Export Cipher Suites Supported (Logjam) | The remote host supports a set of weak ciphers. | Low | Moderata |
| 83875 | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) | The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. | Low | Moderata |
| 153953 | SSH Weak Key Exchange Algorithms Enabled | The remote SSH server is configured to allow weak key exchange algorithms. | Low | Moderata |
| 10407 | X Server Detection | An X11 server is listening on the remote host | Low | Moderata |
| 71049 | SSH Weak MAC Algorithms Enabled | The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms. | Low | Moderata |