Report Dirigante

Come specificato questo è un report sintetizzato sulle problematiche riscontrate verso i vostri sistemi.

CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability

Questi sono gli eventi più critici che sono stati rilevati a cui bisognerebbe dare la priorità per una corretta sicurezza nei sistemi.

- Mancanza di autorizzazioni
- Possibilità di un attacco Informatico
- Cifratura di chiavi private
- Violazione e furto di dati sensibili

A cui bisogna riporre al più presto rimedio.

MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	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	57582	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 andWeakened 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
MEDIUM	Injection4.3*	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW			
	3.7	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported
LOW	(Logjam)2.6*	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	71049	SSH Weak MAC Algorithms
LOW	Enabled		
	2.6*	10407	X Server Detection

Qui invece sono le vulnerabilità di secondo livello, ma non meno importanti, perché potrebbero comunque creare un problema al sistema se non peggiorare se risolte. Possiamo trovare problemi come:

- Debug delle connessoni al Web Server
- Non corretto trasferimento dei dati
- Mancanza di certificazioni di sicurezza
- Mancato controllo sui certificati di sicurezza
- Criptografia debole