



Traccia:

A partire dal report di ieri:

- Analisi/studio delle vulnerabilità (PDF) - servirà sia per exploit che remediation
 - Report PDF per «dirigente»
 - Inteso come riassunto che va presentato ai dirigenti per l'approvazione a livello finanziario ecc.
- Non contiene troppi dettagli tecnici ma soltanto l'indicazione della vulnerabilità e soprattutto i grafici con la pericolosità delle varie vulnerabilità riscontrate

Svolgimento:

CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
----------	-----	---	--------	--

CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
----------	------	---	--------	-------------------------------

Soluzione : Richiede un aggiornamento di Apache Tomcat – Potenzialmente impattante

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
----------	-----	---	-------	-------------------------------

Soluzione : Può essere richiesta reinstallazione

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)
----------	-------	-----	-------	---

Soluzione : Il materiale sensibile coinvolto è da considerarsi non più sottoposto a sicurezza crittografica

CRITICAL	10.0*	-	61708	VNC Server 'password' Password
----------	-------	---	-------	--------------------------------

Soluzione : Sostituzione password con una efficace – Intervento rapido

CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
----------	------	---	-------	---

Soluzione : Richiede aggiornamento del sistema – Intervento impattante

MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate

Soluzione : Acquisto di un certificato SSL – Intervento rapido