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

Apache Tomcat A JP Connector Request Injection (Ghostcat)
Livello di Rischio: CRITICO
Descrizione: Questa vulnerabilità apre la porta a possibili accessi non autorizzati al nostro sistema da parte di terze parti. È necessario un intervento tempestivo per mitigare questo rischio.

Bind Shell Backdoor Detection
Livello di Rischio: CRITICO
Descrizione: Questa rilevazione indica la possibilità di un accesso non autorizzato al nostro sistema attraverso un backdoor. È essenziale adottare misure per prevenire qualsiasi compromissione della sicurezza.

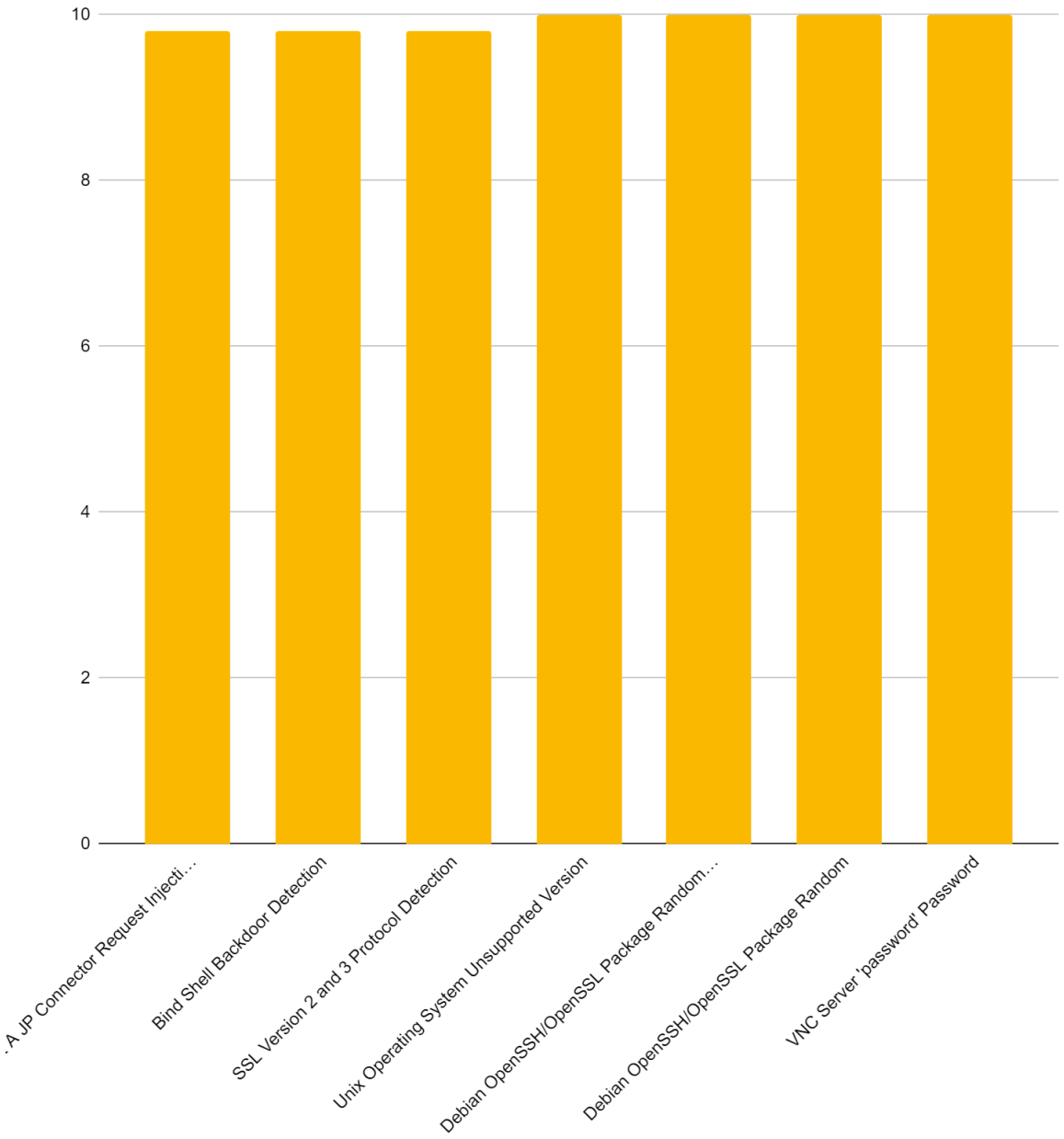
SSL Version 2 and 3 Protocol Detection
Livello di Rischio: CRITICO
Descrizione: L'individuazione di questi protocolli obsoleti può esporre il nostro sistema a vulnerabilità di sicurezza note. È importante adottare protocolli più sicuri per proteggere le nostre comunicazioni.

Unix Operating System Unsupported Version Detection
Livello di Rischio: CRITICO
Descrizione: La presenza di una versione non supportata del sistema operativo Unix rende il nostro sistema vulnerabile a possibili attacchi. È necessario valutare un aggiornamento o un'altra azione correttiva.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Livello di Rischio: CRITICO
Descrizione: Questa debolezza nel generatore di numeri casuali può compromettere la sicurezza delle nostre comunicazioni. È fondamentale adottare misure per garantire l'integrità dei nostri sistemi.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
Livello di Rischio: CRITICO
Descrizione: Una variante della precedente debolezza che coinvolge il controllo SSL. È importante prestare particolare attenzione a questo problema per proteggere le nostre comunicazioni.

VNC Server 'password' Password
Livello di Rischio: CRITICO
Descrizione: La presenza di una password di default o debole per il server VNC costituisce una grave vulnerabilità. È necessario adottare misure per rafforzare la sicurezza del nostro sistema.



Nel grafico a istogramma allegato, ogni barra rappresenta una specifica vulnerabilità, mentre sull'asse verticale è indicata la frequenza con cui queste vulnerabilità si verificano. È fondamentale notare che il punteggio di gravità associato a ciascuna vulnerabilità varia da 0 a 10, dove 10 rappresenta il livello massimo di criticità.

Evidenziando questo punto cruciale, le barre più alte nel grafico corrispondono alle vulnerabilità classificate con un punteggio di gravità 10. Queste rappresentano le minacce più gravi per la sicurezza del sistema e richiedono un'azione immediata.

Interventi di mitigazione:

Apache Tomcat A JP Connector Request Injection (Ghostcat):
Applicare immediatamente le patch di sicurezza fornite da Apache per risolvere questa vulnerabilità.
Configurare in modo sicuro il server Apache Tomcat, ad esempio disabilitando le funzionalità non necessarie e limitando l'accesso ai componenti sensibili.

Bind Shell Backdoor Detection:
Identificare e rimuovere il backdoor dal sistema.
Rivedere e rafforzare le politiche di accesso per prevenire l'accesso non autorizzato.

SSL Version 2 and 3 Protocol Detection:
Disabilitare i protocolli SSL Version 2 e 3 e abilitare solo protocolli TLS più sicuri.
Aggiornare i certificati SSL/TLS e configurare correttamente le suite crittografiche supportate.

Unix Operating System Unsupported Version Detection:
Aggiornare il sistema operativo Unix a una versione supportata e regolarmente aggiornata.
Implementare misure di sicurezza aggiuntive come il monitoraggio dei registri di sistema e l'analisi delle vulnerabilità.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness:
Applicare le patch fornite dai fornitori Debian per correggere la debolezza nel generatore di numeri casuali.
Aggiornare i pacchetti OpenSSH/OpenSSL alla versione più recente.

VNC Server 'password' Password:
Cambiare immediatamente la password del server VNC e utilizzare una password complessa e unica.
Configurare correttamente le autorizzazioni di accesso al server VNC per ridurre i rischi di accesso non autorizzato.