S5-L3

NESSUS

Nessus è un software di scansione delle vulnerabilità, sviluppato da Tenable, Inc., utilizzato per identificare vulnerabilità, configurazioni errate e software obsoleto nei dispositivi e nelle reti. Impiegato da professionisti della sicurezza e amministratori di sistema, rileva criticità come porte aperte, versioni obsolete dei software, vulnerabilità zero-day e problemi di conformità.

Funzioni principali di Nessus:

- Scansione delle vulnerabilità: rileva minacce e configura avvisi di criticità.

- Identificazione di servizi e sistemi operativi: individua i servizi attivi e OS in uso.

- Analisi delle configurazioni di sicurezza: verifica configurazioni critiche.

- Diversi tipi di scansioni: tra cui di rete, di host locale, e di conformità.

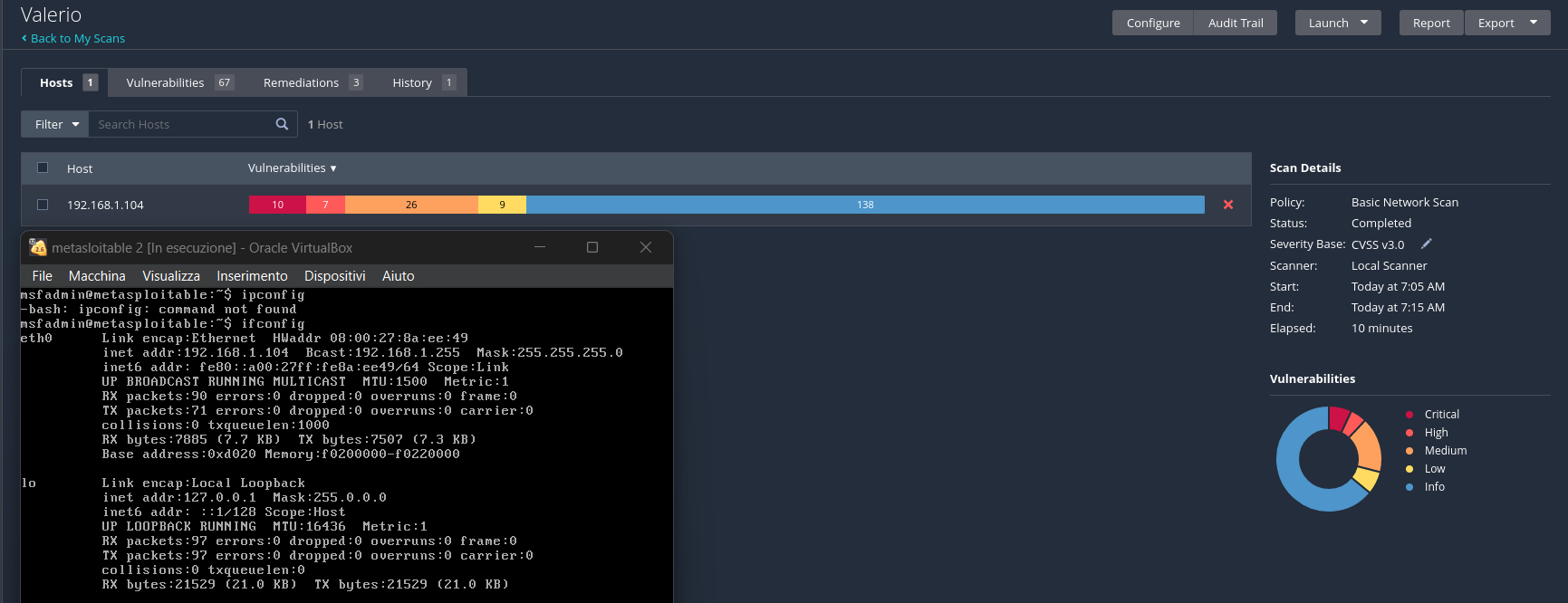
Processi e Vantaggi:

Nessus è facile da configurare e produce report dettagliati classificati per criticità, con indicazioni per la correzione. Le scansioni possono essere reiterate per verificare le risoluzioni. È disponibile nelle versioni Essentials (gratuita), Professional (a pagamento) e in opzioni avanzate (Tenable.io e Nessus Manager).

Vantaggi: interfaccia intuitiva, aggiornamenti frequenti e report dettagliati. Limiti: falsi positivi occasionali e limitazioni nella versione gratuita.

Oggi utilizzeremo la macchina di metasloitable2 per:

* Configurare e avviare scansioni di vulnerabilità con Nessus.
* Analizzare i report di vulnerabilità e comprendere le informazioni fornite.



Utilizzeremo l’ip di metasloitable2 e in automatico il programma nessus scansionerà dopo aver mandato un ping:

* Sistema operativo
* Porte
* Applicazioni
* Registri

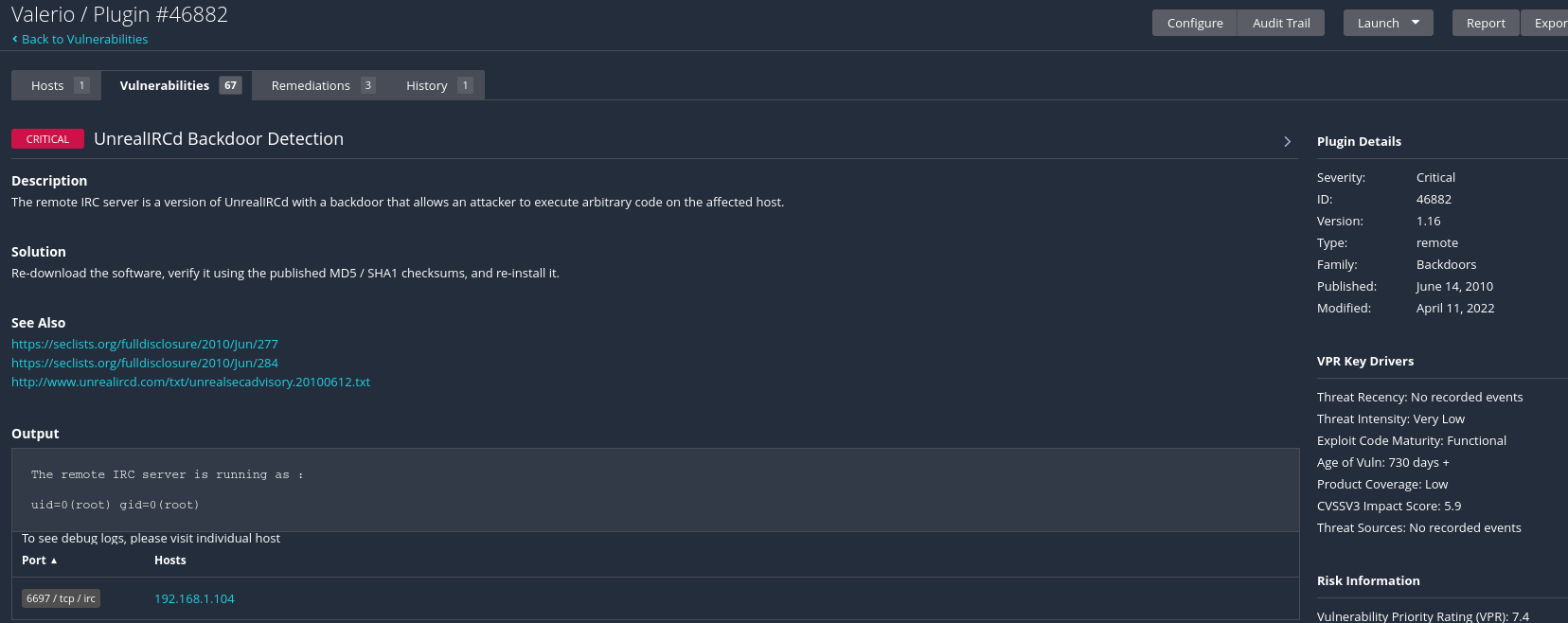
Una volta partita la scansione il programma ( in questo caso impostando su Policy: Basic Network Scan )

Il programma ci darà in risposta le vulnerabilità trovare e quanto sono vulnerabili, nell’esempio troviamo in ordine dal più critico ( critical ) al meno critico ( info):

* 10 critical
* 7 high
* 26 medium
* 9 low
* 138 info

ANALIAZIAMO 5 VULNERABILITA’ PRESE CASUALMENTE

Critical UnrealIRCd Backdoor Detection



La vulnerabilità "Critical UnrealIRCd Backdoor Detection" rilevata da Nessus si riferisce a una grave vulnerabilità di sicurezza che colpisce una versione compromessa del software UnrealIRCd, un popolare server IRC open-source (Internet Relay Chat). Nel 2010, è stata individuata una versione malevola di UnrealIRCd, che conteneva un backdoor intenzionalmente introdotto. Questo backdoor consentiva a un attaccante remoto di eseguire comandi arbitrari sul server senza alcuna autenticazione.

Dettagli della Vulnerabilità

Classificazione: Critica

- Descrizione: La vulnerabilità si verifica perché una versione compromessa di - -- UnrealIRCd era stata distribuita con un backdoor nascosto. Chiunque conosca la backdoor può inviare comandi per ottenere il pieno controllo del sistema in cui UnrealIRCd è installato.

- Accesso per l'Attacco: Da remoto, senza autenticazione.

- Conseguenze: Un attaccante potrebbe ottenere l'accesso completo al server, con possibilità di eseguire comandi di sistema, accedere a file, modificare configurazioni, e potenzialmente installare malware o compromettere ulteriormente la rete.

Impatto

Poiché questa vulnerabilità consente un accesso completo non autenticato, è classificata come \*\*Critica\*\*. Una compromissione di questo tipo potrebbe avere conseguenze serie, tra cui la perdita di dati, l’interruzione dei servizi o l’infezione di altri sistemi nella rete.

Soluzione

La versione compromessa è stata identificata e rimossa dai siti di distribuzione ufficiale di UnrealIRCd, quindi per mitigare la vulnerabilità si consiglia di:

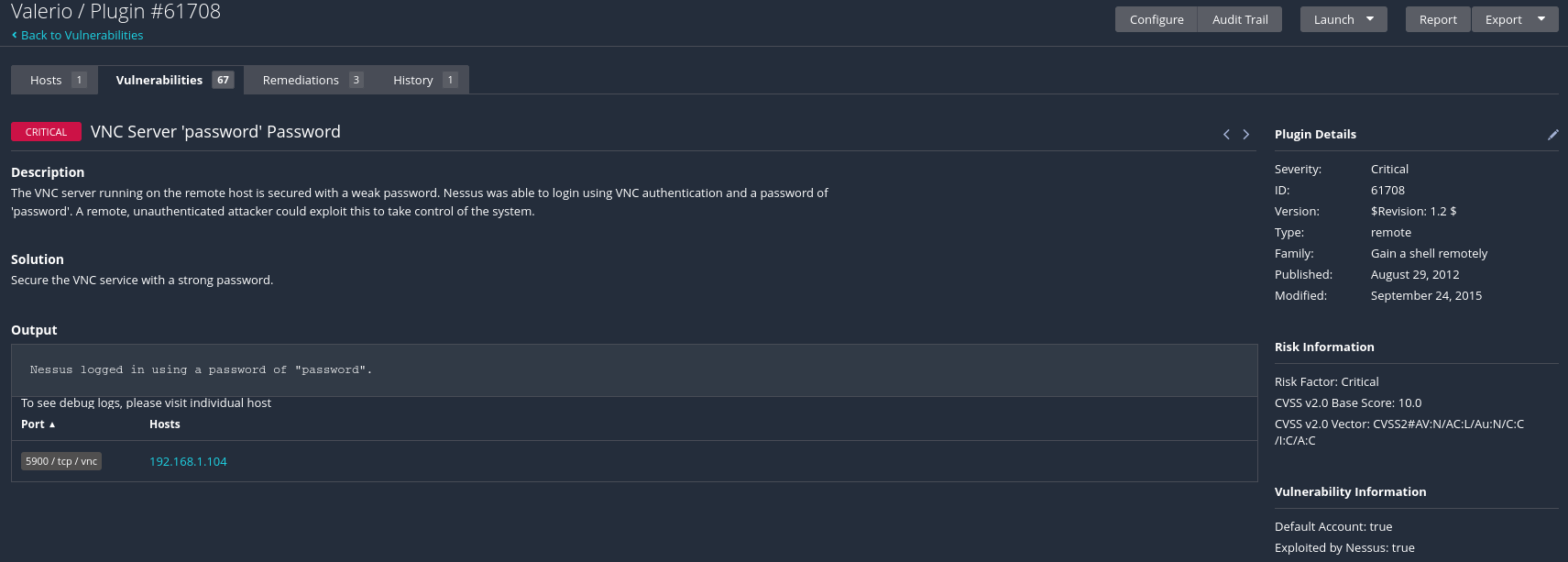
1. Verificare la Versione: Assicurarsi che la versione di UnrealIRCd non sia quella compromessa (versione 3.2.8.1 distribuita prima del 12 giugno 2010).

2. Aggiornare: Installare una versione pulita e aggiornata di UnrealIRCd, scaricandola solo dai siti ufficiali.

3. Rimuovere: Se si rileva una versione compromessa, disinstallarla immediatamente per evitare rischi.

Questa vulnerabilità è rilevata da Nessus poiché la sua criticità può facilmente portare a un compromesso dell’intero sistema.

VNC Server 'password' Password



La vulnerabilità \*\*VNC Server 'password' Password\*\* rilevata da Nessus segnala che un server VNC (Virtual Network Computing) è configurato con una password di autenticazione debole o predefinita (ad esempio, "password"). VNC consente l'accesso remoto a un desktop, quindi una configurazione così debole espone il sistema a rischi di accesso non autorizzato.

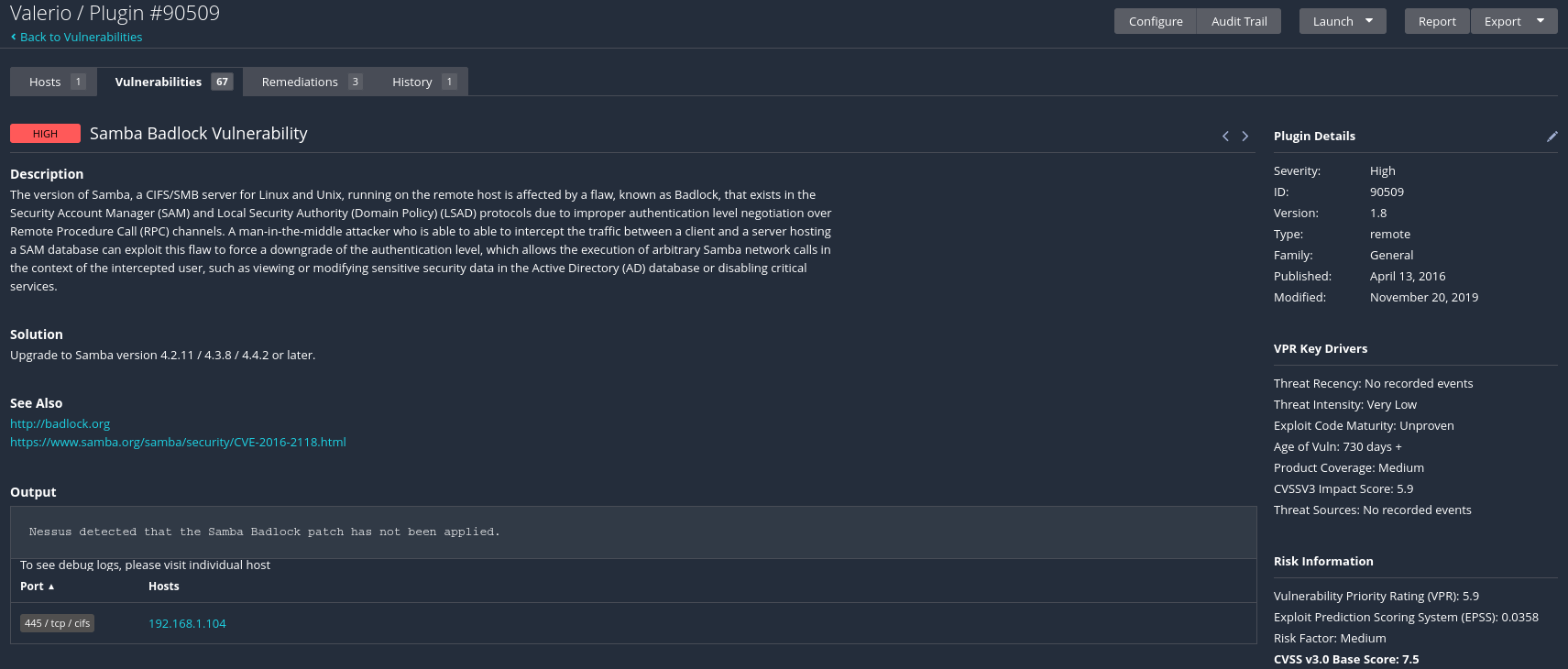
Riepilogo:

- Impatto: Un attaccante potrebbe ottenere l'accesso remoto al sistema, con potenziali conseguenze gravi, come il furto di dati o l'installazione di malware.

- Severità: Alta.

- Mitigazione: Modificare la password VNC con una più complessa, abilitare l’autenticazione a due fattori (se disponibile), e limitare l'accesso VNC a reti sicure o VPN.

vulnerabilità Samba Badlock



La \*\*vulnerabilità Samba Badlock\*\* riguarda un difetto critico di sicurezza nelle versioni di Samba (un software che consente la condivisione di file tra sistemi Linux/Unix e Windows), scoperto nel 2016. Questa vulnerabilità può consentire attacchi di tipo \*\*man-in-the-middle\*\* (MITM) o \*\*Denial of Service (DoS)\*\*, permettendo a un attaccante di intercettare e manipolare il traffico o interrompere i servizi di rete.

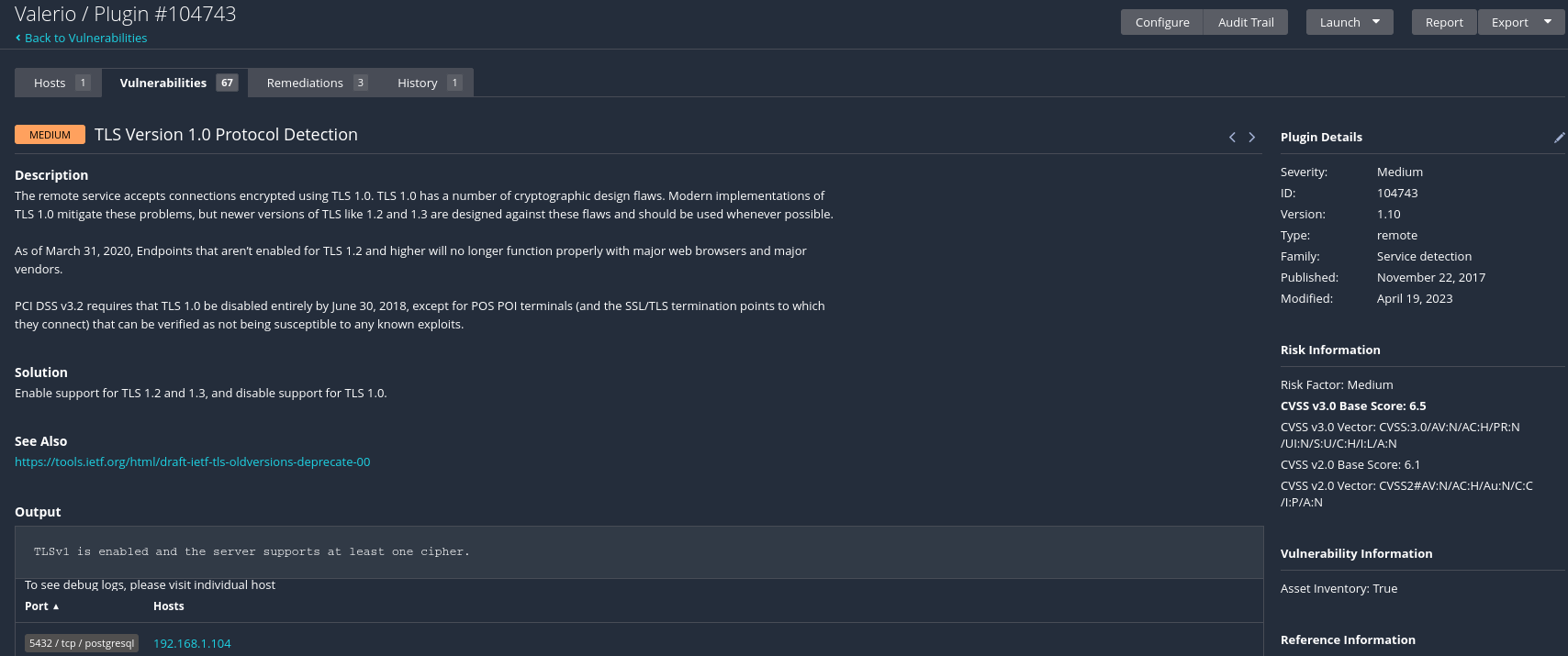
Riepilogo:

- Impatto: Compromissione della comunicazione tra server e client, possibilità di manipolazione dei dati e interruzione dei servizi.

- Severità: Alta.

- Mitigazione: Aggiornare Samba all'ultima versione che risolve il problema; limitare l'accesso ai servizi Samba a reti fidate.

TLS Version 1.0 Protocol Detection



La vulnerabilità \*\*TLS Version 1.0 Protocol Detection\*\* si riferisce alla presenza del protocollo \*\*TLS 1.0\*\* su un server, un protocollo di crittografia considerato obsoleto e insicuro rispetto alle versioni più recenti (come TLS 1.2 e TLS 1.3). TLS 1.0 è vulnerabile a vari attacchi, come \*\*BEAST\*\* e \*\*POODLE\*\*, che possono compromettere la sicurezza delle comunicazioni cifrate.

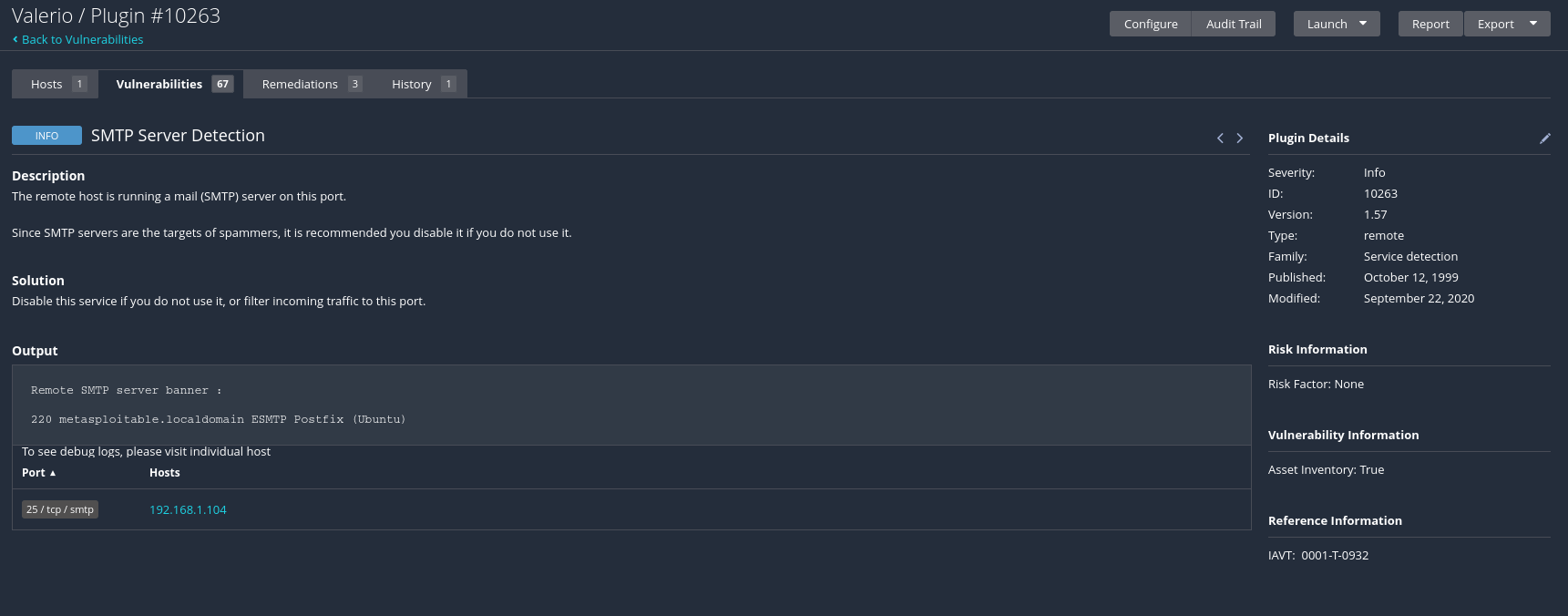
Riepilogo:

- Impatto: Rischio di compromissione dei dati trasmessi, inclusi credenziali e informazioni sensibili.

- Severità: Medio-Alta.

- Mitigazione: Disabilitare TLS 1.0 e forzare l'uso di TLS 1.2 o TLS 1.3. Verificare la compatibilità con i client prima di apportare modifiche per evitare problemi di accesso.

SMTP Server Detection



La vulnerabilità SMTP Server Detection indica che un server SMTP (Simple Mail Transfer Protocol), responsabile dell'invio e della ricezione delle email, è stato rilevato sulla rete durante la scansione. Sebbene non sia di per sé una vulnerabilità, la rilevazione di un server SMTP può fornire informazioni utili a un attaccante per identificare potenziali vettori di attacco, come attacchi di enumerazione degli utenti, spoofing delle email, e relay non autorizzato.

Riepilogo:

- Impatto: Possibili tentativi di abuso del server per spam o attacchi di social engineering.

- Severità: Bassa (a meno che non ci siano configurazioni deboli o vulnerabilità note).

- Mitigazione: Assicurarsi che il server SMTP sia configurato correttamente, abilitando l'autenticazione per evitare relay non autorizzati, e limitare le informazioni fornite nelle risposte SMTP per ridurre il rischio di informazioni sensibili esposte.

REPORT





