SCANSIONE VULNERABILITA

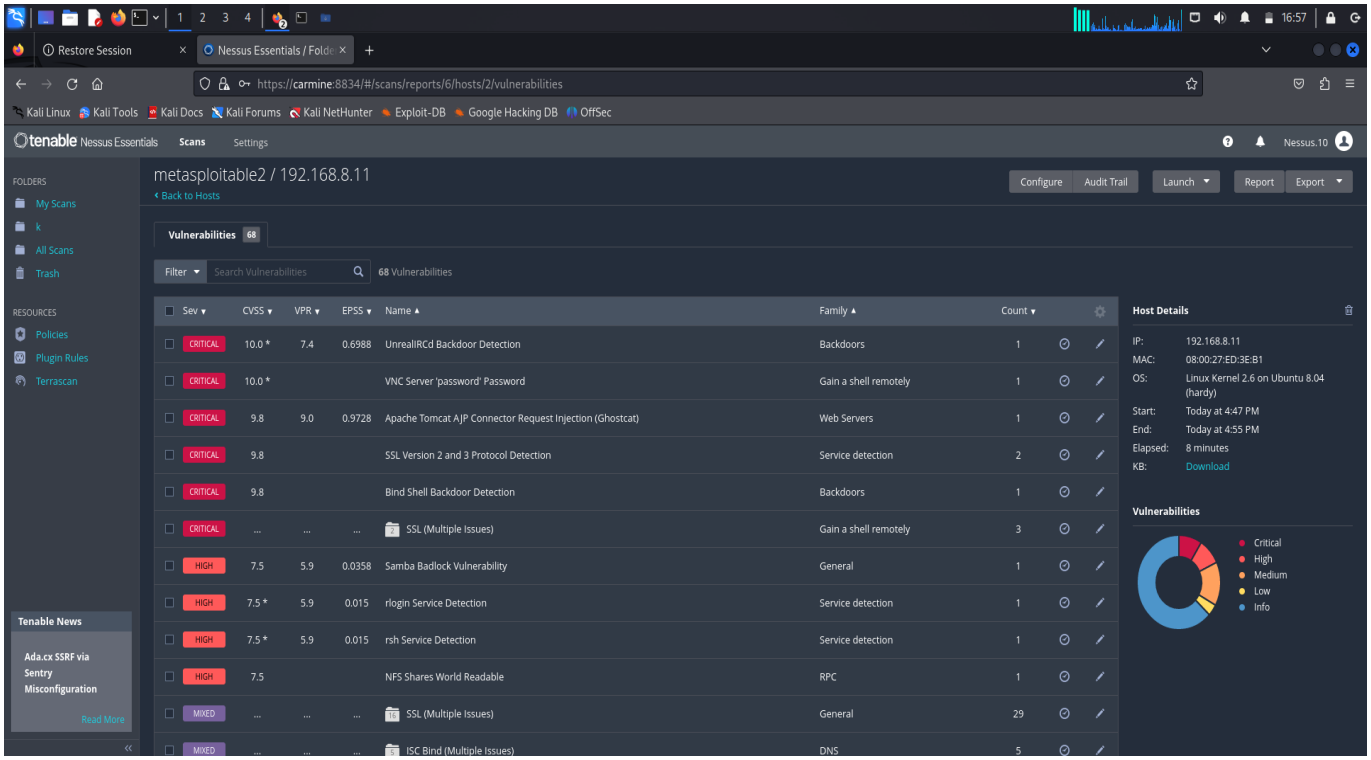
Andremo ad utilizzare Nessus, **Nessus** è uno strumento di fondamentale importanza nel mondo della cybersecurity. È uno **scanner di vulnerabilità** che analizza i tuoi sistemi informatici alla ricerca di possibili punti deboli che potrebbero essere sfruttati da black hacker.

- **Cerca falle:** Esamina attentamente software, sistemi operativi, configurazioni di rete e altri elementi alla ricerca di bug, configurazioni errate e altre vulnerabilità note.
- **Valuta i rischi:** Classifica le vulnerabilità in base alla loro gravità, fornendo informazioni dettagliate su come potrebbero essere sfruttate.
- **Genera report:** Produce report completi e comprensibili che mostrano chiaramente lo stato di sicurezza della tua rete.
- **Si aggiorna costantemente:** Viene continuamente aggiornato con nuove firme di vulnerabilità per garantire la massima protezione.

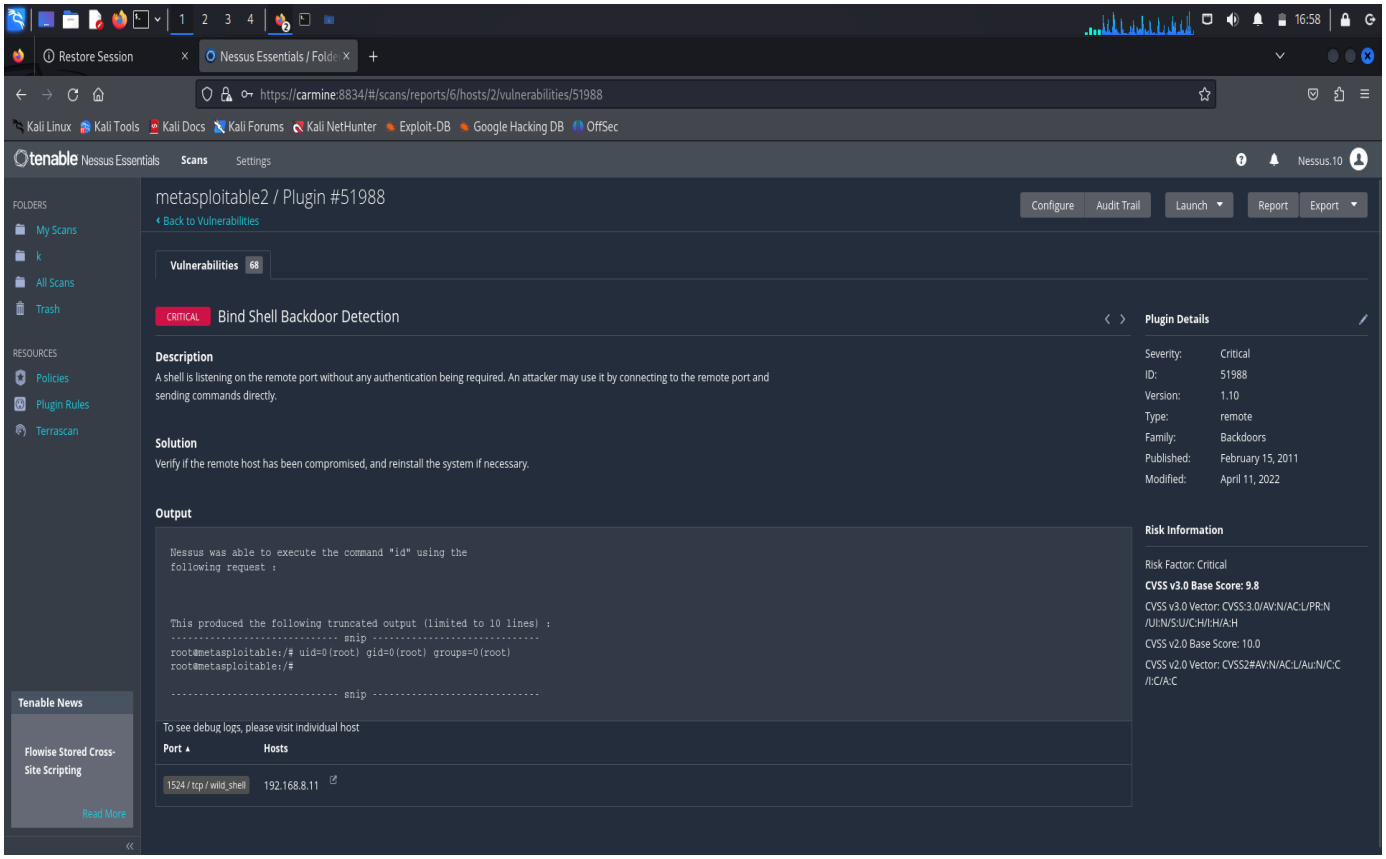
Perché è così importante?

- **Prevenzione degli attacchi:** Identificando le vulnerabilità prima che gli hacker possano sfruttarle, Nessus ti permette di agire in modo proattivo per proteggere i tuoi sistemi.
- **Conformità alle normative:** Molte normative in materia di sicurezza informatica richiedono la scansione periodica delle vulnerabilità. Nessus può aiutarti a soddisfare questi requisiti.
- **Riduzione dei rischi:** Valutando il rischio associato a ciascuna vulnerabilità, puoi prioritizzare le attività di correzione e allocare le risorse in modo efficiente.
- **Miglioramento della sicurezza:** Nessus ti aiuta a mantenere una postura di sicurezza più solida, proteggendo i tuoi dati e la tua reputazione.

Lo scanner ha riscontrato diverse vulnerabilità tra qui 5 critiche.



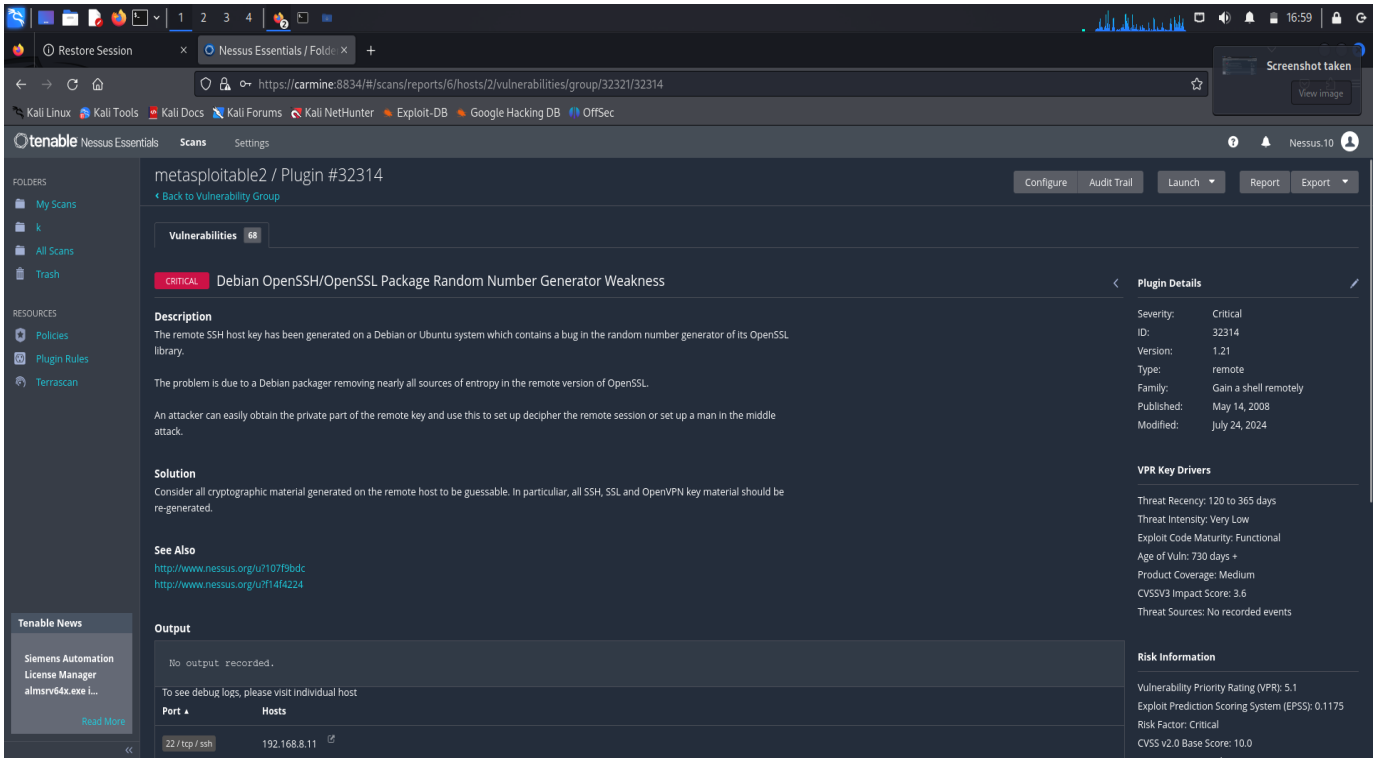
Bind Shell Backdoor Detection



Descrizione:
Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione
Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness



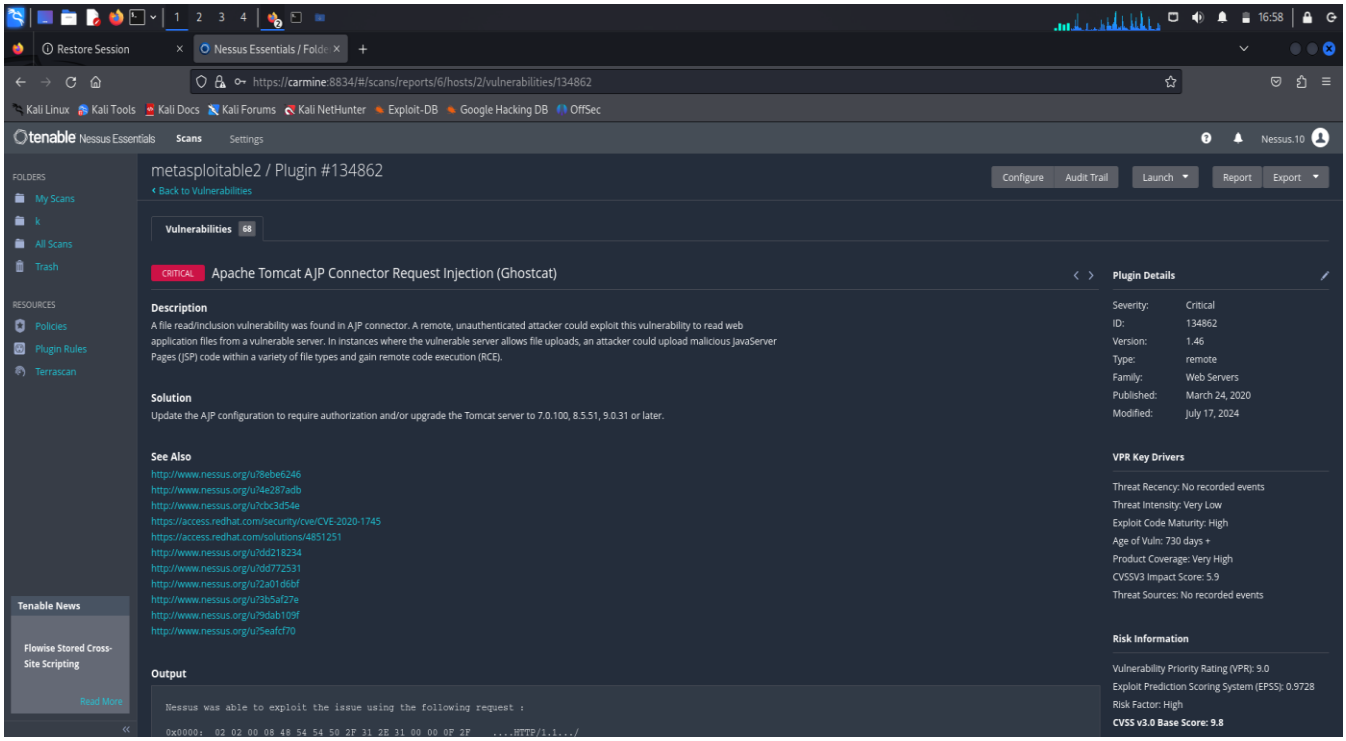
Descrizione:
La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

Soluzione
Considera indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

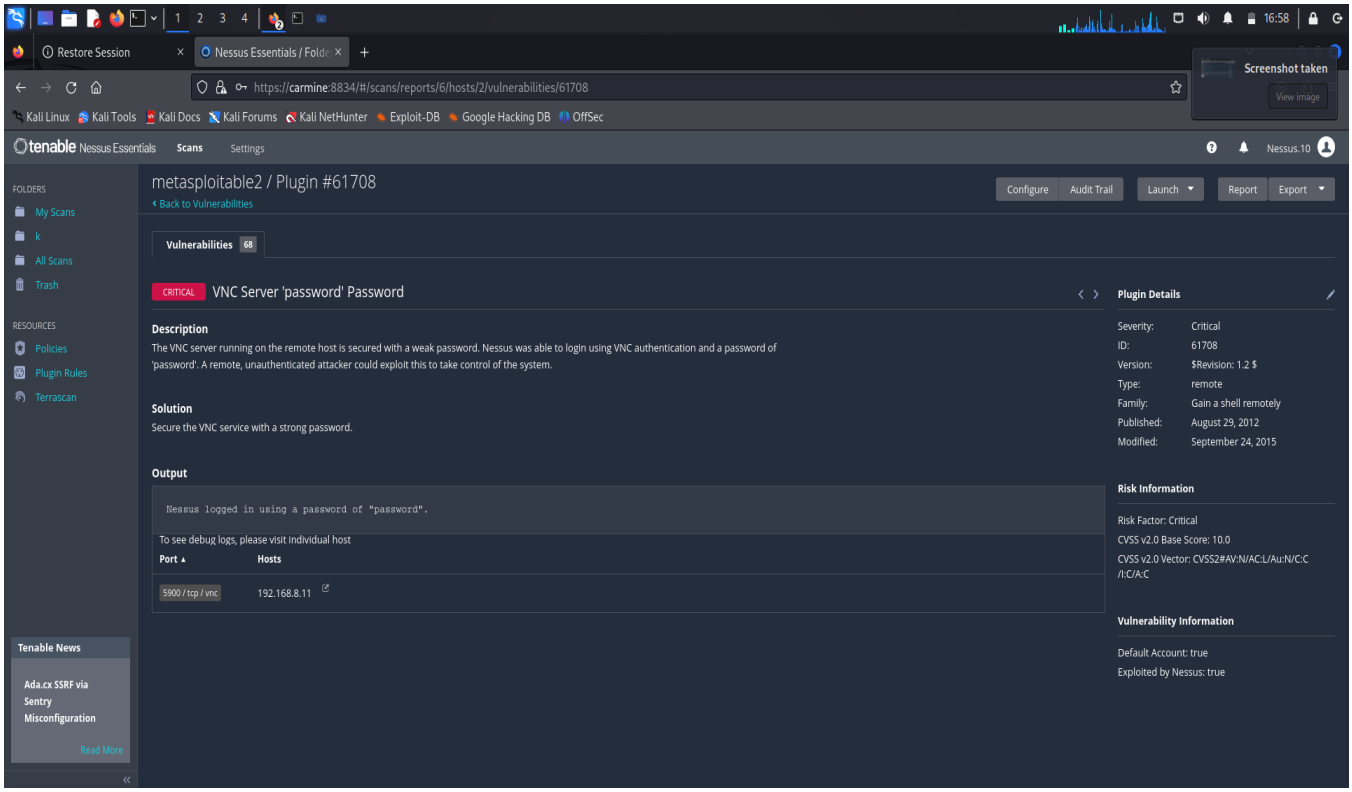
Apache Tomcat AJP Connector Request Injection (Ghostcat)



Descrizione:
È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice in modalità remota (RCE).

Soluzione
Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

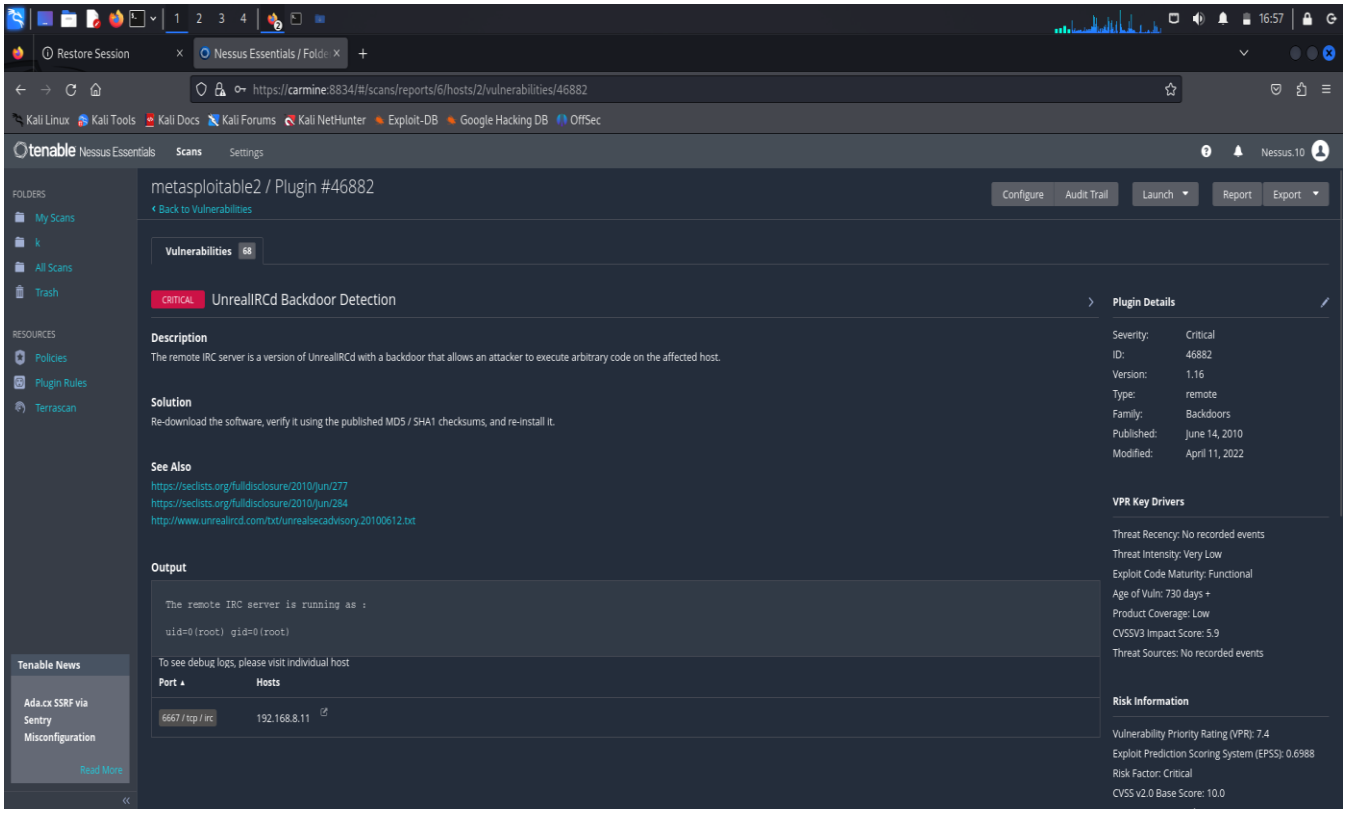
VNC Server 'password' Password



Descrizione:
Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

Soluzione
Proteggi il servizio VNC con una password complessa.

UnrealIRCd Backdoor Detection



Descrizione:
Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato.

Soluzione
Scaricare nuovamente il software, verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.