ivanti

SCHEDA DELLA SOLUZIONE

Dai CVE all'approvazione delle patch

Ora disponibile nelle soluzioni Ivanti per la gestione delle patch

Ivanti permette di accedere ai risultati delle scansioni delle vulnerabilità, visualizzare i CVE (Common Vulnerabilities and Exposures) identificati e le relative patch, quindi pubblicare o approvare le patch mancanti da implementare.

In molti ambienti, i team IT Operations e Security "parlano lingue diverse". Per il team IT Ops, tutto deve funzionare senza intoppi. Il team Security deve proteggere l'ambiente. Ma entrambi condividono lo stesso obiettivo: proteggere l'azienda e promuoverne l'efficienza. E per conseguirlo devono poter collaborare a livello degli endpoint.

Valutazione e risoluzione continua delle vulnerabilità

La valutazione e la risoluzione continua delle vulnerabilità rappresentano un aspetto fondamentale delle pratiche di sicurezza di ogni organizzazione. Ma questo comporta un notevole impegno in termini di tempo e attività manuali dal momento in cui viene individuata una vulnerabilità, fino all'implementazione dell'aggiornamento software necessario per correggerla.

Una singola vulnerabilità è facilmente gestibile, ma un report di vulnerabilità pubblicato dal team Security può contenere 1000, 10.000 o addirittura 50.000 CVE! Una singola valutazione delle vulnerabilità può identificare più problemi sui sistemi dell'intero ambiente, e le stesse vulnerabilità possono esistere in sistemi diversi e in numerosi software su ogni sistema.

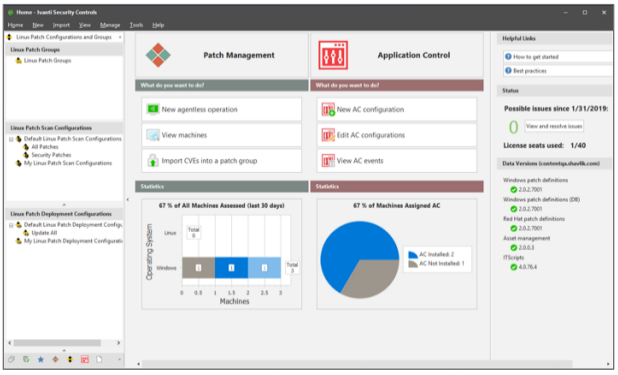
Le attività di valutazione e correzione si traducono quindi in un impegno complesso ed a tempo pieno. Nel frattempo, prima che possano essere implementate le correzioni necessarie, gli hacker ne approfittano per accedere a dati sensibili. Più tempo richiedono le attività di valutazione e correzione, più si resta esposti a violazioni. Il team IT Ops deve esaminare i report ricevuti dal team Security, individuare i CVE, confrontarli con gli aggiornamenti disponibili, e quindi trasmetterli alla soluzione di gestione delle patch.

Ridurre la finestra di tempo tra CVE e patch

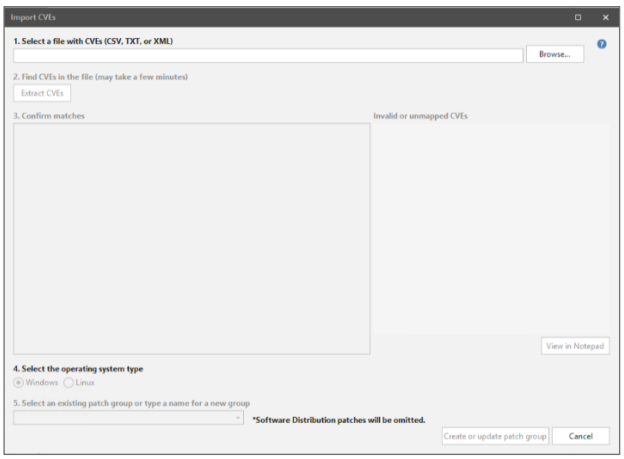
Grazie alle capacità di importazione "da CVE a patch" presenti nelle soluzioni Ivanti, potete semplificare il tutto e ridurre il tempo da diverse ore a pochi minuti. Che si utilizzino le valutazioni delle vulnerabilità di Rapid 7, Tenable, Qualys, BeyondTrust o altri fornitori, le soluzioni Ivanti trovano le patch corrispondenti per tali CVE e generano un elenco di aggiornamenti che potrete quindi approvare o pubblicare rapidamente per proteggere il vostro ambiente.

Uno sguardo alle funzioni

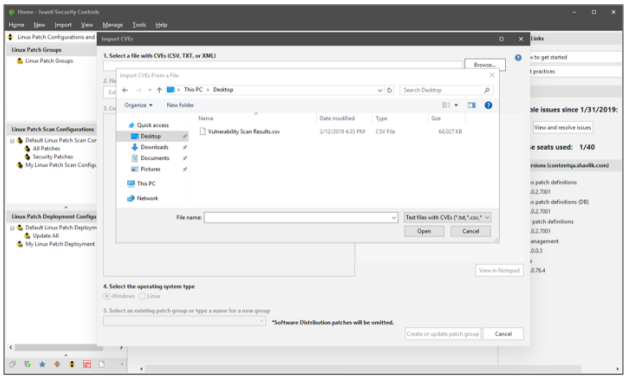
Questa videata illustra la nuova schermata iniziale di Ivanti® Security Controls, in cui potete selezionare "Import CVEs into a Patch Group" (Importa CVE in gruppo di patch).



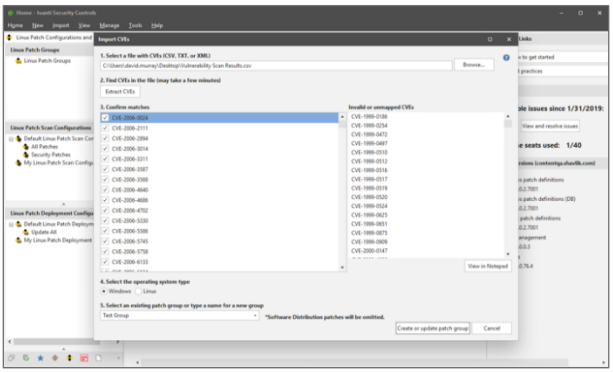
Le informazioni CVE possono essere sotto forma di file XML, CSV da fogli di calcolo o database, o file di testo: la funzione di importazione può gestirli tutti. Le soluzioni Ivanti per la gestione delle patch possono analizzare le informazioni CVE e individuare gli aggiornamenti software necessari per risolvere tali vulnerabilità.



In questa prossima videata, vengono letti i dati CVE contenuti in un file di 64 MB:



Possiamo quindi individuare i CVE, trovare gli aggiornamenti corrispondenti per tali vulnerabilità, e mostrare esattamente quali patch devono essere applicate agli endpoint:



In questo esempio sono stati esaminati 4.880 ID di CVE. Senza questa tecnologia Ivanti, per identificare manualmente i 1369 aggiornamenti associati a tali vulnerabilità avrebbe richiesto diverse ore se non addirittura giorni di ricerca per ogni nuovo report rilasciato dal team Security.

Per saperne di più sulle funzionalità disponibili nelle soluzioni Ivanti per la gestione delle patch, contattate sales@ivanti.com.

Ulteriori informazioni

www.ivanti.it

+39 02 8734 34 21

contact@ivanti.it