CVE: un acronimo importante nella valutazione di prodotti ICT per le aziende

CVE (Common Vulnerabilities and Exposures) è oggi lo standard di riferimento per l'identificazione e la classificazione delle vulnerabilità di sicurezza informatica, benché esistano altri sistemi che svolgono funzioni simili (per esempio NVD, OSVDB, CWE).

CVE presenta diversi vantaggi rispetto ad altri standard, tra cui:

- essere riconosciuto a livello globale;
- essere gestito da un'organizzazione indipendente (*MITRE Corporation*);
- essere gratuito.

Si tratta di un dizionario centralizzato, costantemente aggiornato con tutte le vulnerabilità e le falle di sicurezza riscontrate globalmente nel settore informatico.

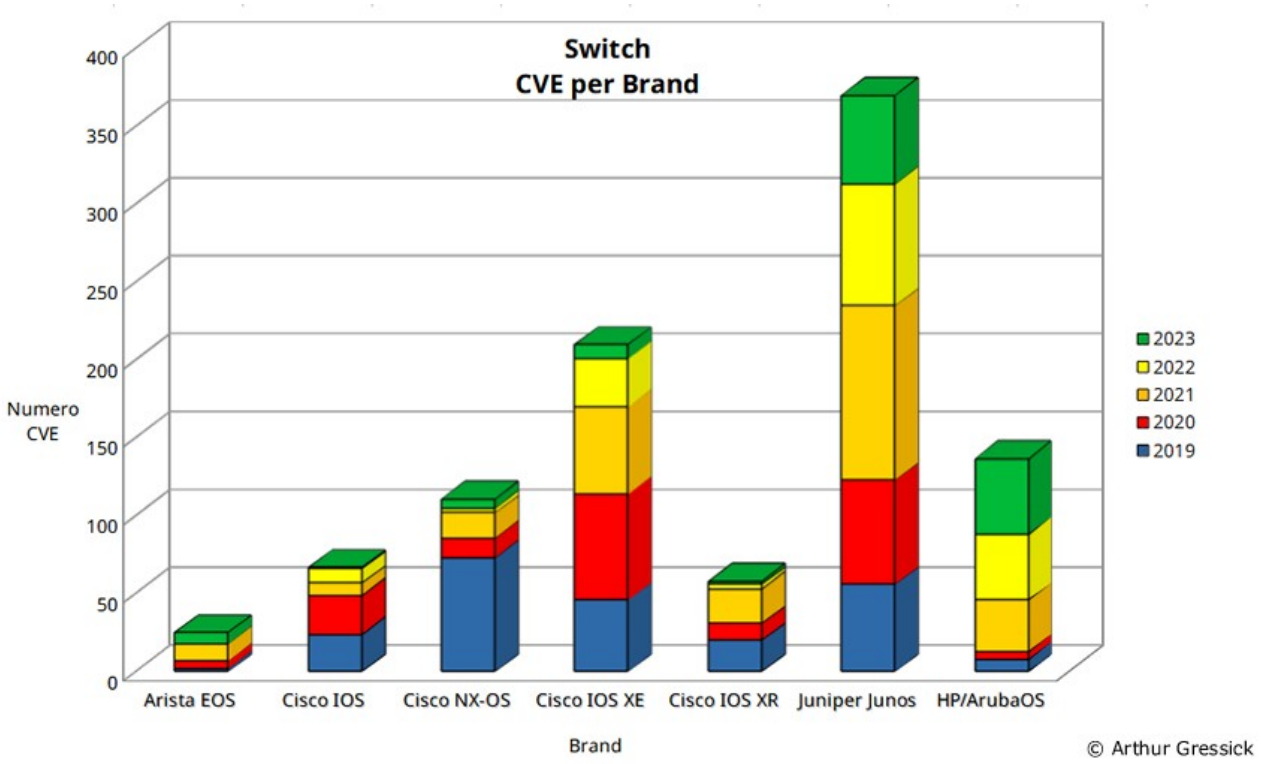
Tale dizionario viene gestito e mantenuto da organizzazioni note come “Autorità di numerazione CVE” (CNA), ovvero autorizzate dal "Programma CVE" ad assegnare "ID CVE" alle vulnerabilità e a pubblicarli.

Gli "ID CVE" (o semplicemente CVE) indicano quindi in modo univoco le vulnerabilità di sicurezza informatica e questo processo di identificazione non genera graduatorie né assegna punteggi a prodotti e produttori.

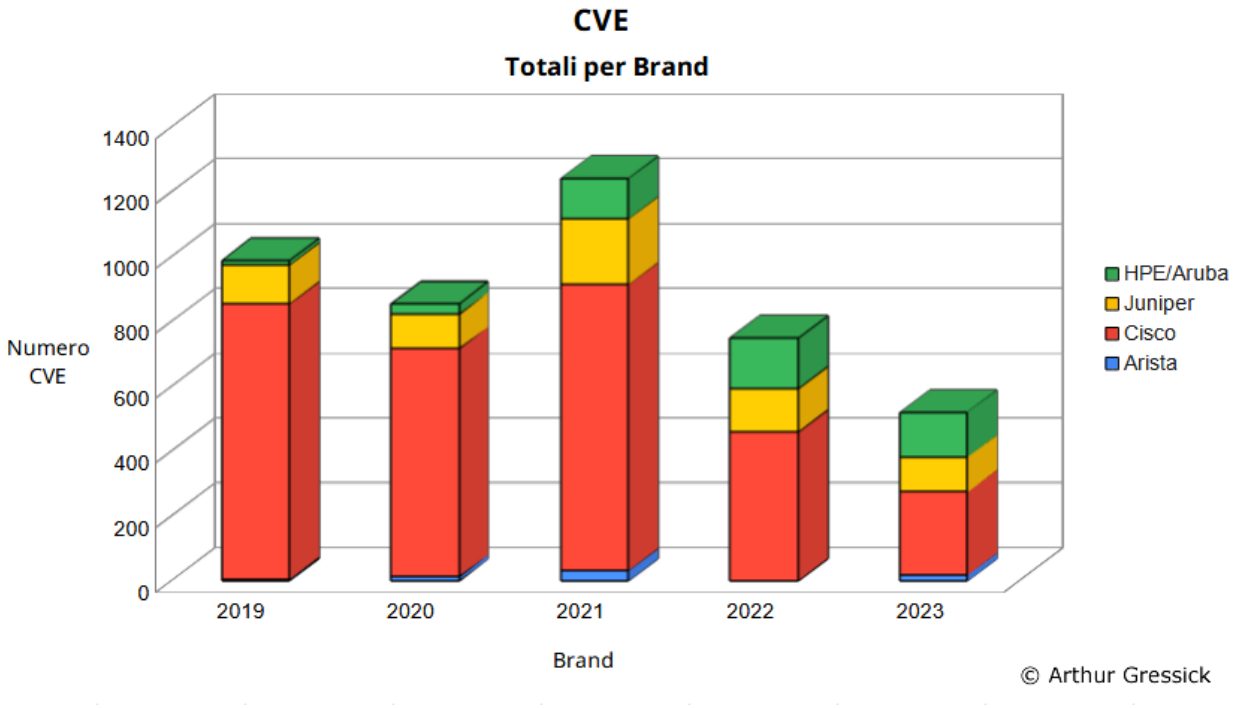
Attualmente ci sono 319 CNA partecipanti al programma CVE, presenti in 37 Paesi: in Italia in particolare è operativo CSIRT (Computer Security Incident response Team), istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN).

CVE è quindi uno strumento fondamentale per la "Cyber Security" che consente di:

- identificare e classificare le vulnerabilità in modo univoco e indipendente dal fornitore o dal prodotto;
- comunicare le vulnerabilità a tutte le parti interessate: produttori, fornitori di software, ricercatori in ambito sicurezza e operatori di rete;
- facilitare la ricerca e accelerare la correzione delle vulnerabilità.



Esempio di CVE per la categoria Switch



CVE totali per Brand di produttori di Switch

Perché CVE è importante per le scelte tecnologiche delle aziende?

Perché rende possibile conoscere, per ogni tipologia di apparato (switch, router, firewall, ecc.) e per le relative aziende produttrici, il numero di CVE generati, ovvero a quante vulnerabilità e falle di sicurezza gli apparati (e i relativi software di sistema e applicativi) sono stati soggetti.

In un momento storico in cui gli attacchi informatici si sono moltiplicati esponenzialmente, diventando sempre più sofisticati, conoscere il numero di CVE che hanno afflitto un prodotto e il suo "brand" è una variabile non più trascurabile nella valutazione di un acquisto.

Una variabile che influenza solo l'acquisto iniziale?

Un CVE è un allarme e come tale deve essere sempre preso in seria considerazione da chi lo riceve: gli addetti alla sicurezza informatica aziendale, i consulenti, i fornitori in outsourcing, ecc.

Le loro analisi, da effettuarsi nel più breve tempo possibile, verificheranno la gravità del possibile impatto sull'infrastruttura e dovranno portare celermente allo svolgimento di attività: applicare al più presto gli aggiornamenti di sicurezza disponibili e verificare se la vulnerabilità possa causare, o abbia già causato, danni che potrebbero peggiorare propagandosi nell'infrastruttura o che piuttosto possano riflettersi sull'immagine aziendale (siti web, posta elettronica) o innescare problematiche di carattere legale (GDPR, danni a Clienti o soggetti terzi).

La "variabile CVE" influisce dunque non solo sui costi iniziali di acquisto (certi) ma anche su quelli successivi di gestione, indiretti e soprattutto imprevedibili (blocchi dell'attività aziendale, perdita di dati).

Quando si programma un investimento tecnologico in azienda è quindi consigliabile tenere in conto anche questo essenziale parametro, per evitare di incorrere, sopravvalutando il solo criterio “costo di acquisto”, in significativi costi operativi generati da continui interventi correttivi sugli apparati inseriti nella propria infrastruttura informatica.

I grafici inseriti in questo articolo riportano i CVE relativi ad una classe di apparati e ad alcuni brand e sono stati estratti da un'approfondita analisi fatta da Arthur Gressick che potete scaricare a questo link.

Link:

- CVE
- CVE CNE Partner
- CSIRT
- Arista Networking
- IPnext

#CVE #CyberSecurity #IPnext