Cisco IOS XE Web UI Vulnerability

Ottobre 2023

Report Informativo SOC

Dettagli documento

Titolo attività
Cisco IOS XE Web UI Vulnerability

Sintesi attività
Report contenente le evidenze relative all'attacco ai router Cisco IOS XE che sfrutta la vulnerabilità CVE-2023-20198 per installare un impianto che consente di eseguire comandi malevoli con privilegi elevati.

Destinatario pubblicazione
Referenti servizi SOC e SOC AdS

Livello di riservatezza (Clear/Green/Amber/Amber+Strict/Red)
CLEAR

Data pubblicazione
18/10/2023

Redatto da
Mirko Ioris

Revisionato da
Massimo Giaimo

Riservatezza della pubblicazione

Al documento viene applicato un livello di riservatezza, avvalorato dalla voce “Livello di riservatezza” presente in prima pagina. I valori utilizzabili (RED / AMBER / GREEN / CLEAR) hanno i seguenti significati:

TLP:RED = Riservato ai soli partecipanti.

> Le fonti possono utilizzare TLP:RED quando le informazioni non possono essere efficacemente utilizzate da altre parti e potrebbero avere un impatto sulla privacy, sulla reputazione o sulle operazioni di una parte se utilizzate in modo improprio. I destinatari non possono condividere le informazioni TLP:RED con parti al di fuori dello specifico scambio, riunione o conversazione in cui sono state originariamente divulgate. Nel contesto di una riunione, ad esempio, le informazioni di TLP:RED sono limitate ai presenti alla riunione. Nella maggior parte dei casi, TLP:RED dovrebbe essere scambiato verbalmente o di persona.

TLP:AMBER = Divulgazione limitata, riservata alle organizzazioni dei partecipanti.

TLP:AMBER+STRICT limita la condivisione solo all'*organizzazione*.

> Le fonti possono utilizzare TLP:AMBER quando le informazioni richiedono supporto per agire in modo efficace, ma comportano rischi per la privacy, la reputazione o le operazioni se condivise al di fuori delle organizzazioni coinvolte. I destinatari possono condividere le informazioni TLP:AMBER solo con i membri della propria organizzazione e con clienti o clienti che hanno bisogno di conoscere le informazioni per proteggersi o prevenire ulteriori danni.
>
> Nota: se la fonte desidera limitare la condivisione **solo** all'organizzazione, deve specificare TLP:AMBER+STRICT.

TLP:GREEN = Divulgazione limitata, riservata alla comunità.

> Le fonti possono utilizzare TLP:GREEN quando le informazioni sono utili per la consapevolezza di tutte le organizzazioni partecipanti, nonché con i colleghi all'interno della comunità o del settore più ampio. I destinatari possono condividere le informazioni TLP:GREEN con colleghi e organizzazioni partner all'interno del loro settore o comunità, ma non tramite canali pubblicamente accessibili. Le informazioni in questa categoria possono essere ampiamente diffuse all'interno di una particolare comunità. Le informazioni TLP:GREEN potrebbero non essere rilasciate al di fuori della community.

TLP:CLEAR = La divulgazione non è limitata.

Le fonti possono utilizzare TLP:CLEAR quando le informazioni comportano un rischio minimo o prevedibile di uso improprio, in conformità con le regole e le procedure applicabili per il rilascio pubblico. Fatte salve le norme standard sul copyright, le informazioni TLP:CLEAR possono essere distribuite senza restrizioni.

Indice

Introduzione

Lunedì 16 ottobre 2023 Cisco ha riportato che una vulnerabilità critica zero-day è stata sfruttata per creare backdoor nei dispositivi che eseguono il software Cisco IOS XE esposti su internet.

Questa vulnerabilità, tracciata con l'id **CVE-2023-20198** [1] e classificata come critica con un punteggio CVSS di 10/10, consente a un aggressore remoto non autenticato di creare un account con privilegi elevati sul sistema vulnerabile e utilizzarlo per prendere il controllo del sistema stesso.

La vulnerabilità riguarda sia dispositivi fisici che virtuali con l'interfaccia web HTTP o HTTPS attiva.

Panoramica sull'attacco

La prima istanza di attività malevola è stata rilevata a fine settembre da Cisco [2], quando un indirizzo IP sospetto (**5.149.249[.]74**) è riuscito a creare un account locale denominato **cisco_tac_admin** su un sistema vulnerabile. Si tratta probabilmente di un test iniziale da parte del threat actor.

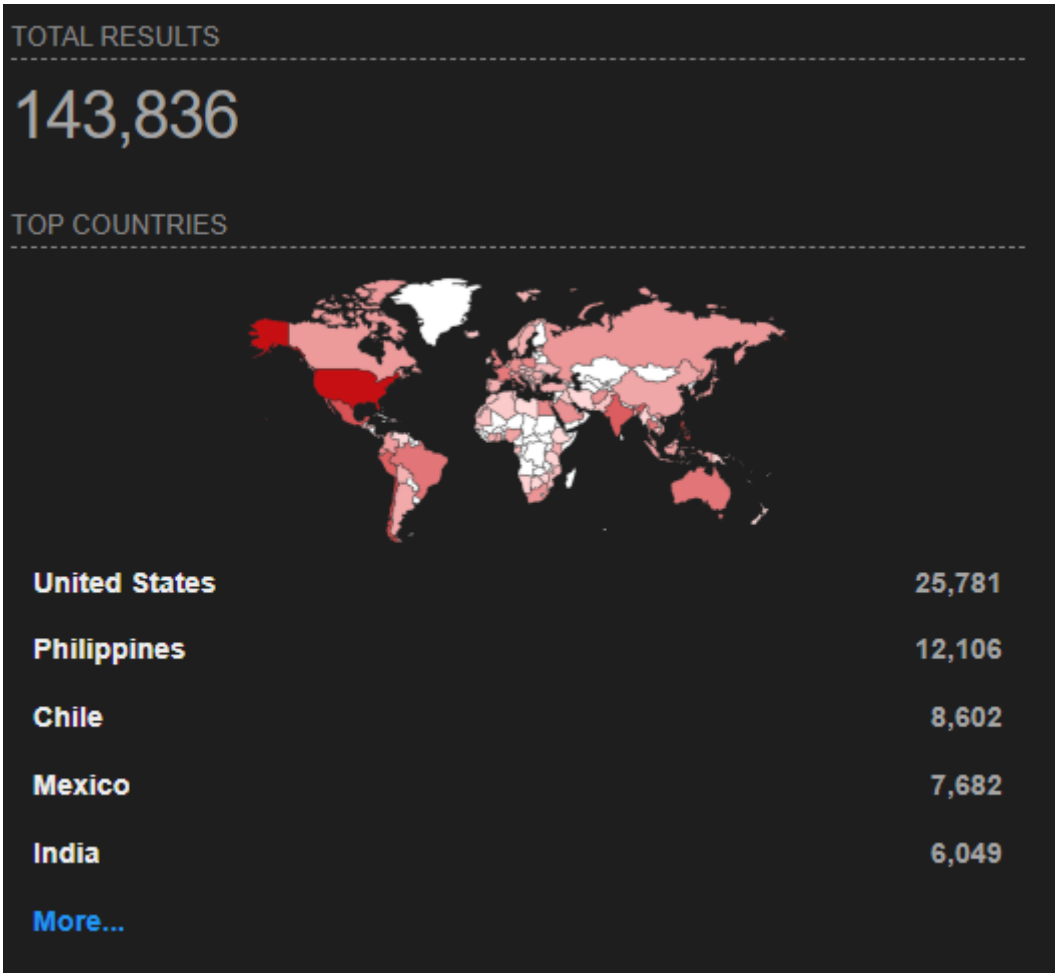
Un secondo tentativo è stato osservato da un altro indirizzo IP (**154.53.56[.]231**), che ha creato un account chiamato **cisco_support** e lo ha utilizzato per impiantare un file sul sistema, **usr/binos/conf/nginx-conf/cisco_service.conf**. Il file di configurazione è stato utilizzato per definire un nuovo endpoint del server web che può essere usato dall'attaccante per eseguire comandi arbitrari a livello di sistema.

Da quanto è stato osservato finora, affinché l'impianto diventi attivo e l'attaccante ottenga il controllo completo, è necessario riavviare il server web. Questo significa che gli host compromessi che non sono ancora stati riavviati non sono al momento sotto controllo degli attaccanti.

Superficie d'attacco

Attraverso un motore di ricerca per dispositivi come Shodan è possibile controllare la quantità di dispositivi Cisco IOS XE esposti su internet con l'interfaccia web attiva e dunque potenzialmente vulnerabili.

Il risultato è allarmante, con più di 140mila dispositivi esposti a livello globale, di cui **1.598** solo in Italia.



E' stata utilizzata una dork condivisa su Twitter dal CEO di Aves Netsec [3]

Alcune attività di verifica della superficie già compromessa da queste azioni ha permesso al momento di identificare circa **30.000** dispositivi già attaccati con successo.

L'azienda **Vulncheck** ha condiviso su GitHub [4] uno scanner per rilevare la presenza dell'impianto malevolo sui dispositivi vulnerabili

Secondo le analisi condotte dal Cyber Security Team di Wuerth Phoenix la percentuale di host compromessi, a livello italiano, è il **16,65%** del totale.

Come proteggersi

E' di vitale importanza agire velocemente e controllare se i propri dispositivi sono stati compromessi. Al momento non esiste alcuna patch ufficiale che risolve la vulnerabilità CVE-2023-20198, è dunque fortemente raccomandato **disabilitare l'interfaccia web** dei sistemi Cisco IOS XE esposti su internet.

IoC

IP:

5.149.249[.]74

154.53.56[.]231

Username:

cisco_tac_admin

cisco_support

Bibliografia

[1]https://nvd.nist.gov/vuln/detail/CVE-2023-20198

[2]https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

[3]https://twitter.com/SimoKohonen/status/1714213806371479849

[4]https://github.com/vulncheck-oss/cisco-ios-xe-implant-scanner