

Riepilogo della pubblicazione semestrale del bundle Cisco IOS e IOS XE Software Security Advisory, 25 settembre 2019

'+'[Top of the section](#)'+''); } function endA() { //alert("end"); document.write('

'); } function startExpandIndentSubheader() { document.write('

'); } function endExpandIndentSubheader() { document.write('

'); } function endIndent() { //alert("end"); document.write('

'+'+'[Expand all sections](#)'+' '+'[Collapse all sections](#)'+'+'+'[Close Section](#)'+'

ID advisory: cisco-sa-20190925-bundle

<https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20190925-bundle>

Revisione 1.0

Per la release pubblica 2019 settembre 25 15:30 UTC (GMT)

Sommario

[Riepilogo](#)

[Versioni e correzioni software](#)

[Come ottenere software fisso](#)

[Stato della notifica: Finale](#)

[Distribuzione](#)

[Cronologia delle revisioni](#)

[Procedure di sicurezza di Cisco](#)

[Riepilogo](#)

Cisco ha pubblicato la sua pubblicazione semestrale Cisco IOS e IOS XE Software Security Advisory Bundled il 25 settembre 2019. In risposta diretta al feedback dei clienti, Cisco rilascia i pacchetti di Cisco IOS e IOS XE Software Security Advisories il quarto mercoledì del mese, in marzo e settembre di ogni anno solare.

La release del 25 settembre 2019 della pubblicazione Cisco IOS e IOS XE Software Security Advisory Bundled include 12 Cisco Security Advisories che descrivono 13 vulnerabilità nel software Cisco IOS e nel software Cisco IOS XE. Cisco ha rilasciato aggiornamenti software che risolvono queste vulnerabilità.

Tutte le vulnerabilità hanno un indice di impatto sulla sicurezza (SIR) elevato. Il corretto sfruttamento delle vulnerabilità potrebbe consentire all'autore di un attacco di ottenere un accesso

non autorizzato, condurre un attacco tramite comando injection o causare una condizione di negazione del servizio (DoS) su un dispositivo interessato.

Due delle vulnerabilità influiscono sia sul software Cisco IOS che sul software Cisco IOS XE. Due delle vulnerabilità riguardano il software Cisco IOS, mentre otto riguardano il software Cisco IOS XE. Una delle vulnerabilità influisce sull'ambiente dell'applicazione Cisco IOx. Cisco ha confermato che nessuna delle vulnerabilità influisce sul software Cisco IOS XR o Cisco NX-OS.

Per determinare rapidamente se una specifica versione del software Cisco IOS o IOS XE è interessata da una o più vulnerabilità, utilizzare Cisco IOS Software Checker.

[Versioni e correzioni software](#)

Per gli aggiornamenti del software, consultare anche il sito <http://www.cisco.com/go/psirt> e le eventuali avvertenze successive per determinare l'esposizione e una soluzione di aggiornamento completa.

In ogni caso, i clienti devono fare attenzione a che i dispositivi da aggiornare contengano memoria sufficiente e che le attuali configurazioni hardware e software continuino a essere supportate correttamente dalla nuova release. Se le informazioni non sono chiare, contattare il Cisco Technical Assistance Center (TAC) o il provider di servizi di manutenzione autorizzato per assistenza.

[Come ottenere software fisso](#)

Cisco ha rilasciato aggiornamenti software che risolvono queste vulnerabilità. Prima di distribuire il software, i clienti devono consultare il proprio fornitore di manutenzione o verificare la compatibilità del software con le funzionalità e i problemi noti specifici del proprio ambiente.

I clienti possono installare solo i set di funzionalità acquistati e ottenere il supporto richiesto. Installando, scaricando, accedendo o utilizzando in altro modo tali aggiornamenti software, i clienti accettano di essere vincolati dai termini delle condizioni di licenza software Cisco disponibili all'indirizzo http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html o come altrimenti stabilito all'indirizzo Cisco.com Download all'indirizzo <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> .

Non contattare psirt@cisco.com o security-alert@cisco.com per gli aggiornamenti del software.

[Clienti con contratti di assistenza](#)

I clienti con contratti devono ottenere il software tramite i canali di aggiornamento regolari. Per la maggior parte dei clienti, le patch software e le correzioni dei bug devono essere ottenute tramite il

Software Center sul sito Web di Cisco all'indirizzo <http://www.cisco.com>.

[Clienti che utilizzano organizzazioni di supporto di terze parti](#)

I clienti i cui prodotti Cisco vengono forniti o mantenuti tramite accordi precedenti o esistenti con organizzazioni di supporto di terze parti, quali partner Cisco, rivenditori autorizzati o fornitori di servizi devono contattare tale organizzazione di supporto per ricevere assistenza e supporto relativamente alla linea di azione appropriata in relazione a questo avviso.

L'efficacia di qualsiasi soluzione o correzione dipende dalle situazioni specifiche del cliente, ad esempio dal mix di prodotti, dalla topologia di rete, dal comportamento del traffico e dalla missione aziendale. A causa della varietà di prodotti e versioni interessate, i clienti devono consultare il proprio provider di servizi o l'organizzazione di supporto per assicurarsi che qualsiasi soluzione o correzione applicata sia la più appropriata per l'utilizzo nella rete prevista prima che venga implementata.

[Clienti senza contratti di assistenza](#)

I clienti che acquistano direttamente da Cisco ma non sono in possesso di un contratto di assistenza Cisco e i clienti che acquistano tramite fornitori di terze parti ma non sono riusciti a ottenere software fisso tramite il punto vendita devono ottenere patch software e correzioni di bug contattando il Cisco Technical Assistance Center (TAC). I contatti TAC sono i seguenti.

- +1 800 553 2447 (numero verde dal Nord America)
- +1 408 526 7209 (chiamata gratuita da qualsiasi parte del mondo)
- email: tac@cisco.com

I clienti devono avere a disposizione il proprio numero di serie del prodotto ed essere pronti a fornire l'URL di questo avviso come prova del diritto a una patch software o a una correzione di bug. I clienti senza contratto di assistenza devono richiedere una patch software o una correzione di bug tramite il TAC.

Per ulteriori informazioni sui contatti TAC, compresi i numeri di telefono localizzati, le istruzioni e gli indirizzi e-mail, consultare il sito http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html.

[Stato della notifica: Finale](#)

IL PRESENTE DOCUMENTO VIENE FORNITO "COSÌ COM'È" E NON IMPLICA ALCUNA GARANZIA O CONCESSIONE, INCLUSE LE GARANZIA DI COMMERCIALIZZABILITÀ O IDONEITÀ PER UNO SCOPO SPECIFICO. L'UTILIZZO DA PARTE DELL'UTENTE DELLE INFORMAZIONI CONTENUTE NEL DOCUMENTO O NEI MATERIALI ACCESSIBILI DAL DOCUMENTO AVVIENE A PROPRIO RISCHIO. CISCO SI RISERVA IL DIRITTO DI MODIFICARE O AGGIORNARE IL PRESENTE DOCUMENTO IN QUALSIASI MOMENTO.

Una copia standalone o una parafrasi del testo di questo documento che omette l'URL di distribuzione nella sezione seguente è una copia non controllata e può non contenere informazioni importanti o contenere errori materiali.

Distribuzione

Questo avviso è pubblicato sul sito Web mondiale di Cisco all'indirizzo:

<https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20190925-bundle>

Oltre ai messaggi Web internazionali, una versione di testo di questo avviso è chiaramente firmata con il codice PGP di Cisco PSIRT e viene inviata ai seguenti destinatari di e-mail e news Usenet.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- fulldisclosure@seclists.org
- comp.dcom.sys.cisco@newsgate.cisco.com

Eventuali aggiornamenti futuri di questo avviso saranno pubblicati sul sito Web mondiale di Cisco, ma potranno essere annunciati attivamente nelle mailing list o nei newsgroup. Gli utenti interessati al problema sono invitati a controllare l'URL sopra indicato per eventuali aggiornamenti.

Cronologia delle revisioni

Prima pubblicazione: 25 settembre 2019

Stato: Finale

Version: 1.0

Procedure di sicurezza di Cisco

Le informazioni complete sulla segnalazione delle vulnerabilità della sicurezza nei prodotti Cisco, su come ottenere assistenza in caso di incidenti relativi alla sicurezza e su come registrarsi per

ricevere informazioni sulla sicurezza da Cisco, sono disponibili sul sito Web di Cisco all'indirizzo http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html. Ciò include istruzioni per richieste di informazioni sulla sicurezza Cisco. Tutti gli avvisi sulla sicurezza Cisco sono disponibili all'indirizzo <http://www.cisco.com/go/psirt>.