Riepilogo della pubblicazione semestrale del bundle Cisco IOS e IOS XE Software Security Advisory, 28 settembre 2016

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

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

'+"+"'+'+'[Expand all sections]'+' '+' [Collapse all sections]'+'+'"+'+'Close Section'+'

ID advisory: cisco-sa-20160928-bundle

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160928-bundle

Revisione 1.0

Per la Pubblica Release 2016 Settembre 28 16:00 UTC (GMT)

Sommario

Riepilogo

La release del 28 settembre 2016 della pubblicazione Cisco IOS e IOS XE Software Security Advisory Bundled include 10 Cisco Security Advisories che descrivono 11 vulnerabilità nel software Cisco IOS e IOS XE. Per un elenco completo degli avvisi e dei relativi collegamenti, vedere Cisco Event Response: Pubblicazione semestrale del bundle Cisco IOS e IOS XE Software Security Advisory, settembre 2016.

Versioni e correzioni software

Cisco ha rilasciato aggiornamenti software gratuiti che risolvono le vulnerabilità descritte in questa pubblicazione fornita con il pacchetto.

Come ottenere software fisso

Cisco ha rilasciato aggiornamenti software gratuiti che risolvono le vulnerabilità descritte in questa pubblicazione fornita con il pacchetto. I clienti possono installare e richiedere supporto solo per le versioni software e i set di funzionalità per cui hanno acquistato una licenza. Installando, scaricando, accedendo o utilizzando in altro modo tali aggiornamenti software, i clienti accettano di rispettare i termini della licenza software Cisco:
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Inoltre, i clienti possono scaricare solo software per cui dispongono di una licenza valida, acquistato da Cisco direttamente o tramite un rivenditore o partner autorizzato Cisco. Nella maggior parte dei casi si tratta di un aggiornamento di manutenzione del software acquistato in precedenza. Gli aggiornamenti gratuiti del software di protezione non danno diritto a nuove licenze software, a set di funzionalità software aggiuntivi o ad aggiornamenti di revisioni importanti.

Quando si prendono in considerazione aggiornamenti software, i clienti devono consultare regolarmente gli avvisi per i prodotti Cisco, disponibili nella pagina Avvisi e avvertenze sulla sicurezza Cisco, per determinare l'esposizione e una soluzione di aggiornamento completa.

In ogni caso, i clienti devono accertarsi 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, si consiglia ai clienti di contattare il Cisco Technical Assistance Center (TAC) o i provider di manutenzione sotto contratto.

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 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 terzi ma non sono riusciti a ottenere software fisso tramite il punto vendita devono ottenere gli aggiornamenti contattando il Cisco Technical Assistance Center (TAC):
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

I clienti devono avere a disposizione il numero di serie del prodotto ed essere pronti a fornire l'URL di questo avviso come prova del diritto a un aggiornamento gratuito.

Stato della notifica: Finale

IL PRESENTE DOCUMENTO VIENE FORNITO "COSÌ COM'È" E NON IMPLICA ALCUNA GARANZIA O CONCESSIONE, INCLUSE LE GARANZIA DI COMMERCIABILITÀ 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 potrebbe non contenere informazioni importanti o contenere errori materiali. Le informazioni di questo documento sono destinate agli utenti finali dei prodotti Cisco.

Distribuzione

Il presente avviso è disponibile al seguente indirizzo:
http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160928-bundle

Inoltre, una versione testuale della presente notifica è firmata in modo non crittografato con il codice PGP (Cisco Product Security Incident Response Team (PSIRT) e inviata ai seguenti destinatari di e-mail e news Usenet:

- bugtraq@securityfocus.com
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco@newsgate.cisco.com
- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- full-disclosure@lists.grok.org.uk
- vulnwatch@vulnwatch.org

Eventuali aggiornamenti futuri del presente avviso verranno pubblicati sul sito Cisco.com, ma potranno essere annunciati o meno sulle mailing list o sui newsgroup. I clienti sono invitati a verificare la disponibilità di aggiornamenti per questa nota all'URL precedente.

Cronologia delle revisioni

Procedure di sicurezza di Cisco

Per 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, vedere Policy di vulnerabilità della sicurezza di Cisco. La policy include anche informazioni di contatto per le pubbliche relazioni e domande della stampa relative alle informazioni sulla vulnerabilità della sicurezza di Cisco.

Tutti i consigli sulla sicurezza di Cisco sono disponibili all'indirizzo http://www.cisco.com/go/psirt.