

# Riepilogo dei consigli sui pacchetti software Cisco IOS, 22 settembre 2010

['+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-20100922-bundle**

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

## Revisione 1.0

Per la versione pubblica 2010 settembre 22 00:00 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](#)

## [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 riportate su <http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN.html> o come altrimenti stabilito su Cisco.com Download su <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Non contattare [psirt@cisco.com](mailto:psirt@cisco.com) o [security-alert@cisco.com](mailto:security-alert@cisco.com) per aggiornamenti 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)
- e-mail: [tac@cisco.com](mailto: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, inclusi i numeri di telefono localizzati, le istruzioni e gli indirizzi di posta elettronica, da utilizzare in diverse lingue, fare riferimento a [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html).

## Stato della notifica: Finale

**Queste informazioni sono altamente riservate di Cisco - Non ridistribuire.**

QUESTA È LA VERSIONE BOZZA DI UNA NOTA SULLA SICUREZZA CHE CONTIENE INFORMAZIONI NON RILASCIATE SUI PRODOTTI CISCO. LA DISTRIBUZIONE ALL'INTERNO DI CISCO È LIMITATA AL PERSONALE CON NECESSITÀ DI SAPERE. QUESTA BOZZA PUÒ CONTENERE ERRORI O OMETTERE INFORMAZIONI IMPORTANTI.

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

## Distribuzione

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

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

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

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)

- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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](#)

## [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](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>.