

Zusammenfassung der Cisco IOS Software Bundled Advisories, 22. September 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 '+'](#)

Beratungs-ID: cisco-sa-20100922-Paket

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

Revision 1.0

Für die Veröffentlichung 2010, 22. September, 00:00 UTC (GMT)

Inhalt

[Zusammenfassung](#)

[Softwareversionen und -korrekturen](#)

[Erwerb fester Software](#)

[Status dieser Mitteilung: Finale](#)

[Distribution](#)

[Revisionsverlauf](#)

[Cisco Sicherheitsverfahren](#)

[Zusammenfassung](#)

[Softwareversionen und -korrekturen](#)

Wenn Sie Software-Upgrades in Erwägung ziehen, wenden Sie sich auch an <http://www.cisco.com/go/psirt> und alle weiteren Ankündigungen, um Informationen zur Verfügbarkeit und einer vollständigen Upgrade-Lösung zu erhalten.

In allen Fällen sollten Kunden darauf achten, dass die zu aktualisierenden Geräte genügend Speicher enthalten und dass die aktuellen Hardware- und Softwarekonfigurationen von der neuen Version weiterhin ordnungsgemäß unterstützt werden. Wenn die Informationen nicht klar sind, wenden Sie sich an das Cisco Technical Assistance Center (TAC) oder Ihren vertraglich

vereinbarten Wartungsanbieter.

Erwerb fester Software

Cisco hat Software-Updates veröffentlicht, die diese Schwachstellen beheben. Vor der Bereitstellung der Software sollten Kunden ihren Wartungsanbieter konsultieren oder die Software auf Kompatibilität der Funktionssätze und auf bekannte umgebungsspezifische Probleme überprüfen.

Kunden dürfen nur die erworbenen Feature-Sets installieren und Unterstützung erwarten. Durch die Installation, das Herunterladen, den Zugriff auf oder die anderweitige Nutzung solcher Software-Upgrades erklären sich Kunden damit einverstanden, an die Bestimmungen der Softwarelizenzbedingungen von Cisco gebunden zu sein, die unter http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html oder unter Cisco.com Downloads unter <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> aufgeführt sind.

Wenden Sie sich bei Software-Upgrades nicht an psirt@cisco.com oder security-alert@cisco.com

Kunden mit Serviceverträgen

Kunden mit Verträgen sollten Software über ihre regelmäßigen Aktualisierungskanäle beziehen. Für die meisten Kunden sollten Software-Patches und Bugfixes über das Software Center auf der weltweiten Website von Cisco unter <http://www.cisco.com> bezogen werden.

Kunden, die Support-Organisationen von Drittanbietern verwenden

Kunden, deren Cisco Produkte im Rahmen von vorherigen oder bestehenden Vereinbarungen mit Drittanbieter-Supportorganisationen wie Cisco Partnern, autorisierten Resellern oder Service Providern bereitgestellt oder gewartet werden, sollten sich an diese Support-Organisation wenden, um Unterstützung bei der geeigneten Vorgehensweise in Bezug auf diese Beratung zu erhalten.

Die Effektivität von Problemumgehungen und Problembehebungen hängt von bestimmten Kundensituationen ab, z. B. Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischen Zielen. Aufgrund der Vielzahl der betroffenen Produkte und Versionen sollten sich Kunden mit ihrem Service Provider oder der Support-Organisation in Verbindung setzen, um sicherzustellen, dass jede angesetzte Problemumgehung oder -behebung für das beabsichtigte Netzwerk am besten geeignet ist, bevor sie bereitgestellt wird.

Kunden ohne Serviceverträge

Kunden, die direkt bei Cisco einkaufen, aber keinen Cisco Servicevertrag abgeschlossen haben, und Kunden, die über Drittanbieter einkaufen, jedoch keine fixe Software über ihren Verkaufsort erhalten, sollten Software-Patches und Fehlerbehebungen erhalten, indem sie sich an das Cisco Technical Assistance Center (TAC) wenden. TAC Kontakte sind wie folgt.

- +1 800 553 2447 (innerhalb Nordamerikas gebührenfrei)
- +1 408 526 7209 (gebührenpflichtiger Anruf von einem beliebigen Standort weltweit)

- E-Mail: tac@cisco.com

Kunden sollten ihre Produktseriennummer zur Verfügung stellen und darauf vorbereitet sein, die URL dieser Benachrichtigung als Nachweis für die Berechtigung zu einem Software-Patch oder einer Fehlerkorrektur anzugeben. Kunden ohne Servicevertrag sollten einen Software-Patch oder eine Fehlerbehebung über das TAC anfordern.

Unter http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html erhalten Sie weitere Kontaktinformationen des TAC, einschließlich lokalisierter Telefonnummern sowie Anleitungen und E-Mail-Adressen für die Verwendung in verschiedenen Sprachen.

Status dieser Mitteilung: Finale

Diese Informationen sind vertrauliche Informationen von Cisco - Nicht weitergeben.

DIES IST EIN ENTWURF EINER SICHERHEITSBENACHRICHTIGUNG, DIE UNVERÖFFENTLICHTE INFORMATIONEN ÜBER CISCO PRODUKTE ENTHÄLT. DIE VERTEILUNG INNERHALB VON CISCO IST AUF PERSONEN BESCHRÄNKT, DIE WISSEN BENÖTIGEN. DIESER ENTWURF KANN FEHLER ENTHALTEN ODER WICHTIGE INFORMATIONEN AUSGEBEN.

DIESES DOKUMENT WIRD "WIE BESEHEN" BEREITGESTELLT UND IMPLIZIERT KEINE GEWÄHRLEISTUNG ODER GEWÄHRLEISTUNG, EINSCHLIESSLICH DER GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT ODER EIGNUNG FÜR EINE BESTIMMTE VERWENDUNG. DIE VERWENDUNG DER INFORMATIONEN IN DEN DOKUMENTEN ODER MATERIALIEN, DIE IM DOKUMENT VERKNÜPFT SIND, ERFOLGT AUF EIGENES RISIKO. CISCO BEHÄLT SICH DAS RECHT VOR, DIESES DOKUMENT JEDERZEIT ZU ÄNDERN ODER ZU AKTUALISIEREN.

Distribution

Diese Ankündigung ist auf der weltweiten Website von Cisco unter folgender Adresse abrufbar:

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

Neben der weltweiten Veröffentlichung über das Internet ist eine Textversion dieser Benachrichtigung mit dem PSIRT PGP-Schlüssel von Cisco eindeutig signiert und wird an die folgenden E-Mail- und Usenet-Nachrichtenempfänger weitergeleitet.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com

- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Künftige Aktualisierungen dieser Sicherheitsberatung werden, falls vorhanden, auf der weltweiten Cisco Website veröffentlicht, können jedoch in Mailinglisten oder Newsgroups aktiv angekündigt werden. Benutzer, die wegen dieses Problems besorgt sind, werden gebeten, die obige URL auf Updates zu überprüfen.

[Revisionsverlauf](#)

[Cisco Sicherheitsverfahren](#)

Umfassende Informationen zur Meldung von Sicherheitsschwachstellen in Cisco Produkten, zum Erhalten von Unterstützung bei Sicherheitsvorfällen und zur Registrierung für den Erhalt von Sicherheitsinformationen von Cisco finden Sie auf der weltweiten Website von Cisco unter http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html. Dazu gehören auch Anweisungen für Presseanfragen zu Cisco Sicherheitsmitteilungen. Alle Cisco Sicherheitsempfehlungen finden Sie unter <http://www.cisco.com/go/psirt>.