

Overzicht van de halfjaarlijkse Cisco IOS-sofwarerelease Adviserende Publicatie, 27 maart 2013

'+'[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](#)'+'

Advies-ID: cisco-sa-20130327-bundel

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20130327-bundle>

Herziening 1.0

Voor de openbare release 2013, 27 maart 16:00 UTC (GMT)

Inhoud

[Samenvatting](#)

[Softwareversies en -bestanden](#)

[Vaste software verkrijgen](#)

[Status van deze kennisgeving: Laatste](#)

[Distributie](#)

[Historie herziening](#)

[Cisco-beveiligingsprocedures](#)

[Samenvatting](#)

Opmerking: De publicatie van 27 maart 2013, Cisco IOS-software Security Adbundelde publicatie, bevat zeven Cisco Security Advisories. Alle advisories aanpakken kwetsbaarheden in Cisco IOS-software. Elk Cisco IOS-sofwarerelease maakt een lijst van de Cisco IOS-sofwarereleases die de kwetsbaarheid of kwetsbaarheden corrigeren die in het advies en de Cisco IOS-sofwarereleases worden beschreven die alle Cisco IOS-sofwarereleases in de bundelde publicatie van maart 2013 corrigeren.

De individuele publicatielink is te vinden in "Cisco Event Response: Semijaarlijks Cisco IOS-sofwarerelease Advies inzake gebundelde publicatie" op de volgende link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

Softwareversies en -bestanden

Bij het overwegen van software-upgrades dient u ook <http://www.cisco.com/go/psirt> te raadplegen en eventuele daaropvolgende adviseurs te raadplegen om de blootstelling en een volledige upgrade-oplossing te bepalen.

In alle gevallen dienen klanten voorzichtig te zijn om er zeker van te zijn dat de apparaten die moeten worden bijgewerkt voldoende geheugen bevatten en dat de huidige hardware- en softwareconfiguraties correct door de nieuwe release zullen worden ondersteund. Als de informatie niet duidelijk is, neemt u contact op met het Cisco Technical Assistance Center (TAC) of uw gecontracteerde onderhoudsprovider voor assistentie.

Vaste software verkrijgen

Cisco heeft software updates vrijgegeven die deze kwetsbaarheden aanpakken. Alvorens software te implementeren dienen klanten hun onderhoudsleverancier te raadplegen of de software te controleren op compatibiliteit met de functieset en bekende problemen die specifiek zijn voor hun omgeving.

Klanten mogen alleen ondersteuning installeren en verwachten voor de door hen aangekochte functiesets. Door dergelijke software-upgrades te installeren, downloaden, gebruiken of anderszins gebruiken, stemmen klanten ermee in gebonden te zijn door de bepalingen van Cisco's softwarelicentie die zijn gevonden op http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html, of zoals anders uiteengezet op Cisco.com Downloads op <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Neem geen contact op met psirt@cisco.com of security-alert@cisco.com voor software-upgrades.

Klanten met servicecontracten

Klanten met contracten moeten software verkrijgen via hun reguliere update-kanalen. Voor de meeste klanten, zouden de softwarepatches en bug-oplossingen via het Software Center op de website van Cisco wereldwijd op <http://www.cisco.com> verkregen moeten worden.

Klanten die ondersteuningsorganisaties van derden gebruiken

Klanten wier Cisco-producten via eerdere of bestaande overeenkomsten met ondersteuningsorganisaties van derden, zoals Cisco-partners, geautoriseerde wederverkopers of serviceproviders, worden geleverd of onderhouden moeten contact opnemen met die ondersteuningsorganisatie voor advies en ondersteuning met de juiste actie voor dit advies.

De effectiviteit van om het even welke tijdelijke oplossing of oplossing is afhankelijk van specifieke klantsituaties, zoals productmix, netwerktopologie, verkeersgedrag en organisatorische missie.

Gezien de verscheidenheid aan getroffen producten en releases moeten klanten hun serviceprovider of ondersteuningsorganisatie raadplegen om te garanderen dat elke toegepaste tijdelijke oplossing of reparatie het meest geschikte is voor gebruik in het bedoelde netwerk voordat deze wordt ingezet.

Klanten zonder servicecontracten

Klanten die direct bij Cisco kopen maar geen Cisco-servicecontract hebben, en klanten die via derden verkopers kopen maar geen vaste software hebben gekregen via hun verkooppunt, moeten softwarepatches en bug-oplossingen verkrijgen door contact op te nemen met het Cisco Technical Assistance Center (TAC). De TAC-contacten zijn als volgt.

- +1 800 553 2447 (gratis vanuit Noord-Amerika)
- +1 408 526 7209 (betaald nummer ergens ter wereld)
- e-mail: tac@cisco.com

Klanten moeten het product serienummer beschikbaar hebben en bereid zijn de URL van deze kennisgeving te verstrekken als bewijs van het recht op een software-pleister of een bug-oplossing. Klanten zonder servicecontracten moeten een softwarepatch aanvragen of een bug in de oplossing zoeken via de TAC.

Raadpleeg http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html voor aanvullende TAC-contactinformatie, inclusief plaatselijke telefoonnummers en instructies en e-mailadressen voor gebruik in verschillende talen.

Status van deze kennisgeving: Laatste

DIT DOCUMENT WORDT AANGEBODEN OP EEN 'AS IS'-BASIS EN IMPLICEERT GEEN ENKEL SOORT GARANTIE, MET INBEGRIIP VAN GARANTIES VAN VERKOOPBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALD DOEL. UW GEBRUIK VAN DE INFORMATIE IN HET DOCUMENT OF DE MATERIALEN GEKOPPELD AAN HET DOCUMENT IS GEHEEL OP EIGEN RISICO. CISCO BEHOUDT ZICH HET RECHT VOOR OM DIT DOCUMENT TE ALLEN TIJDE TE WIJZIGEN OF TE ANNULEREN.

Een zelfstandige kopie of parafrase van de tekst van dit document die de distributie-URL in de volgende sectie weglaat is een ongecontroleerde kopie, en kan belangrijke informatie missen of feitelijke fouten bevatten.

Distributie

Dit advies is beschikbaar op de website van Cisco wereldwijd op:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20130327-bundle>

Naast wereldwijde webpost is een tekstversie van deze bekendmaking duidelijk ondertekend met de Cisco PSIRT PGP-toets en gepost bij de volgende e-mail en nieuwsontvangers van 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
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Eventuele toekomstige updates van dit advies zullen op de website van Cisco wereldwijd worden geplaatst, maar kunnen al dan niet actief worden aangekondigd op mailinglijsten of nieuwsgroepen. Gebruikers die zich zorgen maken over dit probleem worden aangemoedigd om de bovenstaande URL te controleren voor alle updates.

[Historie herziening](#)

[Cisco-beveiligingsprocedures](#)

Volledige informatie over het rapporteren van security kwetsbaarheden in Cisco-producten, het verkrijgen van hulp met veiligheidsincidenten en het registreren om veiligheidsinformatie van Cisco te ontvangen, is beschikbaar op de website van Cisco wereldwijd op http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html. Dit omvat instructies voor persvragen betreffende Cisco veiligheidsmededelingen. Alle Cisco-beveiligingsadviezen zijn beschikbaar op <http://www.cisco.com/go/psirt>.