Overzicht van halfjaarlijkse Cisco IOS en IOS XE-softwarerelease Advies inzake gebundelde publicatie, 23 maart 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'+'

Advies-ID: cisco-sa-20160323-bundel

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160323-bundle

Herziening 1.0

Voor de openbare release 2016-23 maart 16:00 UTC (GMT)

Inhoud

Samenvatting

Bij de publicatie van 23 maart 2016 van Cisco IOS en IOS XE Software Security Advisory Bundled Publication bevat zes Cisco Security Advisories die zes kwetsbaarheden beschrijven. Zie Cisco Event Response voor een volledige lijst met adviseurs en koppelingen naar deze adviseurs: Semijaarlijkse Cisco IOS en IOS XE-softwarerelease Advies inzake gebundelde publicatie.

Softwareversies en -bestanden

Wanneer u softwareupgrades overweegt, worden klanten geadviseerd om het Cisco Security Advisories en Responses archief op http://www.cisco.com/go/psirt te raadplegen en verdere advisories te bekijken om blootstelling en een volledige upgrade-oplossing te bepalen.

In alle gevallen dienen klanten ervoor te zorgen dat de apparaten om te upgraden voldoende geheugen bevatten en te bevestigen dat de huidige hardware- en softwareconfiguraties correct door de nieuwe release zullen worden ondersteund. Als de informatie niet duidelijk is, wordt de klant geadviseerd om contact op te nemen met het Cisco Technical Assistance Center (TAC) of hun gecontracteerde onderhoudsleveranciers.

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 de Cisco-softwarelicentie-bepalingen die op http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html zijn gevonden of zoals anders uiteengezet in 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 van het Software Center op Cisco.com moeten worden verkregen door http://www.cisco.com/cisco/software/navigator.html te bezoeken.

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 aanpak 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 hun product serienummer beschikbaar hebben en bereid zijn om de URL van deze kennisgeving te geven 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 INBEGRIP 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 worldwide:

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160323-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
- fulldisclosure@seclists.org
- comp.dcom.sys.cisco@newsgate.cisco.com

Indien er toekomstige updates van dit advies zullen worden geplaatst op de website van Cisco wereldwijd, 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 veiligheidskwetsbaarheden 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.