Overzicht van de halfjaarlijkse Cisco IOS en IOS XE-softwaresecurity adviespublicaties, 22 maart 2017

'+'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-20170322-bundel

https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20170322-bundle

Herziening 1.0

Voor de openbare release 2017 March 22 16:00 UTC (GMT)

Inhoud

Samenvatting

Dit document maakt deel uit van de publicatie van 22 maart 2017, release van Cisco IOS en IOS XE Software Security Advisory Bundled Publication, die vijf Cisco Security Advisories bevat die vijf kwetsbaarheden beschrijven. Zie Cisco Event Response voor een volledige lijst met de adviseurs en koppelingen naar deze adviseurs: Maart 2017 halfjaarlijks Cisco IOS en IOS XE-softwarerelease Adviserende Publicatie.

Softwareversies en -bestanden

Wanneer u softwareupgrades overweegt, worden de klanten geadviseerd om de adviseurs voor de producten van Cisco regelmatig te raadplegen, die bij de pagina van Cisco Security Advisories en Waarschuwingen beschikbaar zijn, om blootstelling en een volledige upgradeoplossing te bepalen.

In alle gevallen moeten de klanten ervoor zorgen dat de te verbeteren apparaten voldoende geheugen bevatten en 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 de kwetsbaarheden aanpakken die in de adviezen worden beschreven. Klanten mogen alleen ondersteuning installeren en verwachten voor softwareversies en functiesets waarvoor ze een licentie hebben aangeschaft. Door dergelijke software-upgrades te installeren, downloaden, gebruiken of anderszins gebruiken, stemmen klanten ermee in de bepalingen van de Cisco-softwarelicentie te volgen: http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Daarnaast kunnen klanten alleen software downloaden waarvoor ze een geldige licentie hebben, rechtstreeks bij Cisco of via een geautoriseerde wederverkoper of partner van Cisco aangeschaft zijn. In de meeste gevallen gaat het om een onderhoudsupgrade naar software die eerder is aangeschaft. Gratis security software updates geven klanten niet het recht op een nieuwe softwarelicentie, extra software software software-series of belangrijke upgrades.

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 software upgrades via het Software Center op de website van Cisco wereldwijd op http://www.cisco.com moeten worden verkregen.

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, moeten contact opnemen met die ondersteuningsorganisatie voor advies en ondersteuning met de juiste actie voor de adviseurs.

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 rechtstreeks bij Cisco kopen maar geen Cisco-servicecontract hebben en klanten die aankopen via derden leveren maar geen vaste software hebben gekregen via hun verkooppunt, moeten upgrades verkrijgen door contact op te nemen met het Cisco Technical Assistance Center (TAC):
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Klanten moeten over het product-serienummer beschikken en bereid zijn de URL van dit document te geven als bewijs van hun recht op een gratis upgrade.

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 standalone kopie of parafrase van de tekst van dit document die de distributie-URL weglaat is een ongecontroleerde kopie en kan belangrijke informatie missen of feitelijke fouten bevatten. De informatie in dit document is bedoeld voor eindgebruikers van Cisco-producten.

Distributie

Dit document wordt op de website van Cisco worldwide geplaatst op:

https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20170322-bundle

Naast het wereldwijde online posten is een tekstversie van dit document 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-bulletins@lists.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

Indien er toekomstige updates van dit document beschikbaar zijn, zullen deze worden gepubliceerd op de website van Cisco wereldwijd, maar zullen deze 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/c/en/us/about/security-center/security-vulnerability-policy.html. Dit omvat instructies voor persvragen betreffende de informatie van Cisco security kwetsbaarheid. Alle Cisco Security Advisories zijn beschikbaar op http://www.cisco.com/go/psirt.