Overzicht van de halfjaarlijkse Cisco IOS en IOS XE-softwarerelease Advies inzake gebundelde publicatie, 28 september 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-SF-20160928-bundel

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160928-bundle

Herziening 1.0

Voor de openbare release 2016/28 16:00 UTC (GMT)

Inhoud

Samenvatting

Bij de publicatie van 28 september 2016 van Cisco IOS en IOS XE Software Security Advisory Bundled Publication zijn onder meer 10 Cisco Security Advisories ingesloten die 11 kwetsbaarheden in Cisco IOS en IOS XE-software beschrijven. Zie Cisco Event Response voor een volledige lijst met adviseurs en koppelingen naar deze adviseurs: halfjaarlijks Cisco IOS en IOS XE-softwarerelease Advies inzake gebundelde publicatie in september 2016.

Softwareversies en -bestanden

Cisco heeft gratis software updates uitgebracht die de kwetsbaarheden aanpakken die in deze gebundelde publicatie worden beschreven.

Vaste software verkrijgen

Cisco heeft gratis software updates uitgebracht die de kwetsbaarheden aanpakken die in deze gebundelde publicatie 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.

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 dienen klanten ervoor te zorgen dat de apparaten die moeten worden opgewaardeerd 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.

Klanten met servicecontracten

Klanten met contracten moeten software verkrijgen via hun reguliere update-kanalen. Voor de meeste klanten, zouden de softwarepatches en bug-fixes via het Software Center op 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, 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 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 advies te verstrekken als bewijs van het 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 in de volgende sectie 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

Deze mededeling is beschikbaar op de volgende link:
http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160928-bundle

Daarnaast is een tekstversie van deze kennisgeving duidelijk ondertekend met de PGP-toets van het Cisco Product Security Incident Response Team (PSIRT) en naar de volgende e-mailontvangers en Usenet verzonden:

- bugtraq@securityfocus.com
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco@newsgate.cisco.com
- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- full-disclosure@lists.grok.org.uk
- vulnwatch@vulnwatch.org

Eventuele toekomstige updates aan deze kennisgeving zullen aan Cisco.com worden gepubliceerd maar kunnen al dan niet actief worden aangekondigd op mailinglijsten of nieuwsgroepen. Klanten worden aangemoedigd om op de vorige URL te controleren of dit bericht wordt bijgewerkt.

Historie herziening

Cisco-beveiligingsprocedures

Voor 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, zie het Cisco Security kwetsbaarheidsbeleid. Het beleid bevat ook contactinformatie voor public relations en druk op vragen over Cisco security kwetsbaarheidsinformatie.

Alle Cisco Security Advisories zijn beschikbaar op http://www.cisco.com/go/psirt.