Finesse-gadget van derden maakt API-oproepen voor aanvragen mislukken met HTTP 400 na upgrade naar PCCE 15.0.1 SU2

Inhoud

uitgifte

Na het upgraden van PCCE 15.0.1 Finesse van SU1 (15.0.1.10100-104) naar SU2 (15.0.1.10200-61), maken gadgets van derden die de Finesse Gadget API gebruiken de opdracht MakeRequest om agentkenmerken op te halen mislukt met HTTP-statuscode 400 (slecht verzoek). Dezelfde gadgetfunctionaliteit werkt correct wanneer u terugrolt naar SU1. Dit probleem voorkomt dat gadgets van derden succesvolle verzoeken indienen via de Finesse-proxyservice voor gadgets.

Specifieke foutsymptomen zijn onder meer:

- HTTP 400-reacties voor POSTVERZOEKEN naar /gadgets/makeRequest-eindpunt
- Gadgets voor omscholing door externe agent niet langer functioneel
- Aanvragen voor gadgetproxy worden afgewezen als ongeldig

milieu

- Cisco Packaged Contact Center Enterprise (PCCE) 15.0.1
- Finesse opgewaardeerd van SU1 (15.0.1.10100-104) naar SU2 (15.0.1.10200-61)
- Gadgets van derden die gebruikmaken van de Finesse Gadget API makeRequest-functionaliteit
- PCCE-implementatieconfiguraties (2K- en 4K-getest)

resolutie

Dit probleem wordt veroorzaakt door een beveiligingsverbetering die is geïntroduceerd in Finesse 15.0.1 SU2 en die een toegestane poortlijst implementeert voor het verzenden van verzoeken (Cisco bug ID CSCwt62299). De oplossing vereist het configureren van de toegestane poorten waartoe gadgets toegang hebben via de makeRequest API.

Stap 1: Toegestane poorten configureren voor Shindig-aanvragen

Voer deze CLI-opdracht uit op de Finesse-server om de lijst met toegestane poorten te configureren:

```
utils finesse set_property webservices com.cisco.ccbu.finesse.shindig.ssrf.allowed.ports 443,8082,8080,
```

Met deze opdracht wordt het systeem zo geconfigureerd dat gadgetaanvragen naar de opgegeven poorten kunnen worden verzonden. Voeg alle poorten toe waartoe uw gadgets van derden toegang moeten hebben.

Stap 2: Tomcat Service opnieuw starten

Nadat u de toegestane poorten hebt geconfigureerd, start u de Tomcat-service opnieuw op zodat de wijzigingen van kracht worden:

```
utils service restart Cisco Tomcat
```

Stap 3: AW Tomcat opnieuw starten (indien van toepassing)

Als de Tomcat-service AW (Web Application) is uitgeschakeld of opnieuw moet worden gestart, moet u deze ook starten.

Stap 4: Controleer de reset van het wachtwoord voor de gadget van derden

Zorg ervoor dat het wachtwoord van het 3rd-party-gadgetaccount na de upgrade is gereset, omdat dit vereist is voor de gadgetfunctionaliteit van derden. Het wachtwoord moet worden gereset op zowel primaire als secundaire Finesse-servers, indien van toepassing.

Stap 5: Test de functionaliteit van de gadget

Nadat u de configuratiewijzigingen hebt voltooid en de service opnieuw hebt opgestart, test u de gadgetfunctionaliteit van derden om te bevestigen dat MakeRequest API-oproepen nu slagen zonder HTTP 400-fouten.

Oorzaak

Cisco bug ID CSCwt62299. In Finesse 15.0.1 SU2 is een beveiligingsverbetering geïntroduceerd die een toegestane lijst met poorten implementeert voor het verzenden van verzoeken. Deze wijziging voorkomt ongeoorloofde toegang tot systeempoorten door een expliciete configuratie te vereisen van welke poorten gadgets toegang kunnen krijgen via de makeRequest API. Zonder deze configuratie worden alle gadget-proxyverzoeken naar externe URL's geblokkeerd met HTTP 400-fouten als beveiligingsmaatregel tegen potentiële SSRF-aanvallen (Server-Side Request Forgery).

Het oude gedrag stond onbeperkte toegang tot poorten toe voor shinding-verzoeken, terwijl het nieuwe gedrag vereist dat beheerders expliciet definiëren welke poorten toegankelijk zijn om brute-force-aanvallen op open poorten te voorkomen.

Gerelateerde inhoud

- Cisco bug ID CSCwt62299
- Documentatie over migratie van Finesse
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.