Chiamate API makeRequest del gadget di terze parti Finesse non riuscite con HTTP 400 dopo l'aggiornamento a PCCE 15.0.1 SU2

Sommario

Problema

Dopo l'aggiornamento di PCCE 15.0.1 Finesse da SU1 (15.0.1.10100-104) a SU2 (15.0.1.10200-61), i gadget di terze parti che utilizzano il comando Finesse Gadget API makeRequest per recuperare gli attributi dell'agente hanno esito negativo con codice di stato HTTP 400 (richiesta non valida). La stessa funzionalità dei gadget funziona correttamente durante il rollback a SU1. Questo problema impedisce ai gadget di terze parti di effettuare richieste riuscite tramite il servizio proxy dei gadget di Finesse.

I sintomi di errore specifici includono:

- Risposte HTTP 400 per le richieste POST all'endpoint /gadgets/makeRequest
- I gadget per la riqualificazione degli agenti di terze parti non sono più funzionanti
- Richieste proxy di gadget rifiutate come non valide

Ambiente

- Cisco Packaged Contact Center Enterprise (PCCE) 15.0.1
- Finesse è stato aggiornato da SU1 (15.0.1.10100-104) a SU2 (15.0.1.10200-61)
- Gadget di terze parti che utilizzano la funzionalità makeRequest dell'API dei gadget Finesse
- Configurazioni di installazione PCCE (testate a 2K e 4K)

Risoluzione

Questo problema è causato da un miglioramento della sicurezza introdotto in Finesse 15.0.1 SU2 che implementa un elenco di porte consentite per le richieste di condivisione (ID bug Cisco CSCwt62299). La soluzione richiede la configurazione delle porte consentite a cui i gadget possono accedere tramite l'API makeRequest.

Passaggio 1: Configura porte consentite per le richieste di condivisione

Eseguire questo comando CLI sul server Finesse per configurare l'elenco delle porte consentite:

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

Con questo comando viene configurato il sistema per consentire le richieste di gadget alle porte specificate. Includere tutte le porte a cui i gadget di terze parti devono accedere.

Passaggio 2: Riavvia il servizio Tomcat

Dopo aver configurato le porte consentite, riavviare il servizio Tomcat per rendere effettive le modifiche:

```
utils service restart Cisco Tomcat
```

Passaggio 3: Riavviare AW Tomcat (se applicabile)

Se il servizio AW (Application Web) Tomcat non è attivo o deve essere riavviato, avviarlo.

Passaggio 4: Verifica reimpostazione password gadget di terze parti

Verificare che la password dell'account 3rdpartygadget sia stata reimpostata dopo l'aggiornamento, come richiesto per le funzionalità dei gadget di terze parti. La password deve essere reimpostata sui server Finesse primario e secondario, se applicabile.

Passaggio 5: Verifica funzionalità gadget

Dopo aver completato le modifiche alla configurazione e riavviato il servizio, verificare la funzionalità dei gadget di terze parti per verificare che le chiamate all'API makeRequest abbiano esito positivo senza errori HTTP 400.

Causa

Cisco ID bug CSCwt62299. In Finesse 15.0.1 SU2 è stato introdotto un miglioramento della sicurezza che implementa un elenco di porte consentite per la condivisione delle richieste. Questa modifica impedisce l'accesso non autorizzato alle porte di sistema richiedendo una configurazione esplicita delle porte a cui i gadget possono accedere tramite l'API makeRequest. Senza questa configurazione, tutte le richieste del proxy dei gadget agli URL esterni vengono bloccate con errori HTTP 400 come misura di sicurezza contro potenziali attacchi SSRF (Server-Side Request Forgery).

Il vecchio comportamento consentiva l'accesso illimitato alle porte per le richieste di condivisione, mentre il nuovo comportamento richiede agli amministratori di definire in modo esplicito le porte accessibili per impedire attacchi di tipo brute-force sulle porte aperte.

Contenuto correlato

- ID bug Cisco CSCwt6229
- Documentazione sulla migrazione Finesse
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).