Finesse-API-Aufrufe für Make-Request durch Drittanbieter-Gadget schlagen mit HTTP 400 nach dem Upgrade auf PCCE 15.0.1 SU2 fehl

Inhalt

Problem

Nach dem Upgrade von PCCE 15.0.1 Finesse von SU1 (15.0.1.10100-104) auf SU2 (15.0.1.10200-61) schlagen Gadgets von Drittanbietern, die den makeRequest-Befehl der Finesse-Gadget-API verwenden, mit dem HTTP-Statuscode 400 fehl (fehlerhafte Anforderung). Die gleiche Gadget-Funktion funktioniert beim Rollback auf SU1 ordnungsgemäß. Dieses Problem verhindert, dass Gadgets von Drittanbietern erfolgreiche Anforderungen über den Finesse-Gadget-Proxydienst stellen.

Zu den spezifischen Fehlersymptomen gehören:

- HTTP 400-Antworten für POST-Anforderungen an /gadgets/makeRequest-Endpunkt
- Neuzuweisung von Gadgets durch einen Drittanbieter ist nicht mehr möglich
- Die Gadget-Proxyanforderungen werden als ungültig abgelehnt.

Umwelt

- Cisco Packaged Contact Center Enterprise (PCCE) 15.0.1
- Finesse von SU1 (15.0.1.10100-104) auf SU2 (15.0.1.10200-61) aktualisiert
- Drittanbieter-Gadgets mit Finesse Gadget API makeRequest-Funktion
- PCCE-Bereitstellungskonfigurationen (getestet für 2000 und 4000)

Auflösung

Dieses Problem wird durch eine in Finesse 15.0.1 SU2 eingeführte Sicherheitserweiterung verursacht, die eine Liste zulässiger Ports für Shindig-Anforderungen implementiert (Cisco Bug-ID CSCwt62299). Für die Lösung müssen die zulässigen Ports konfiguriert werden, auf die Gadgets über die makeRequest-API zugreifen können.

Schritt 1: Zulässige Ports für Shindig-Anforderungen konfigurieren

Führen Sie diesen CLI-Befehl auf dem Finesse-Server aus, um die Liste der zulässigen Ports zu konfigurieren:

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

Mit diesem Befehl wird das System so konfiguriert, dass Gadget-Anforderungen an die angegebenen Ports zugelassen werden. Schließen Sie alle Ports ein, auf die Ihre Drittanbieter-Gadgets zugreifen müssen.

Phase 2: Tomcat-Dienst neu starten

Starten Sie den Tomcat-Dienst neu, nachdem Sie die zulässigen Ports konfiguriert haben, damit die Änderungen wirksam werden:

```
utils service restart Cisco Tomcat
```

Schritt 3: AW Tomcat neu starten (falls zutreffend)

Wenn der AW (Application Web) Tomcat-Dienst ausgefallen ist oder neu gestartet werden muss, starten Sie ihn ebenfalls.

Schritt 4: Zurücksetzen des Gadget-Kennworts eines Drittanbieters überprüfen

Stellen Sie sicher, dass das Kennwort des 3rdpartygadget-Kontos nach dem Upgrade zurückgesetzt wurde, da dies für die Gadget-Funktionalität eines Drittanbieters erforderlich ist. Das Kennwort muss ggf. sowohl auf dem primären als auch auf dem sekundären Finesse-Server zurückgesetzt werden.

Schritt 5: Test-Gadget-Funktion

Nachdem die Konfigurationsänderungen und der Service neu gestartet wurden, testen Sie die Gadget-Funktionalität des Drittanbieters, um sicherzustellen, dass makeRequest API-Aufrufe jetzt ohne HTTP 400-Fehler erfolgreich sind.

Ursache

Cisco Bug-ID CSCwt62299. In Finesse 15.0.1 SU2 wurde eine Sicherheitserweiterung eingeführt, die eine zulässige Liste von Ports für shindig-Anfragen implementiert. Diese Änderung verhindert den nicht autorisierten Zugriff auf Systemports, da explizit festgelegt werden muss, auf welche Ports Gadgets über die makeRequest-API zugreifen können. Ohne diese Konfiguration werden alle Gadget-Proxy-Anfragen an externe URLs mit HTTP-400-Fehlern blockiert, um die Sicherheit vor potenziellen SSRF-Angriffen (Server-Side Request Forgery) zu gewährleisten.

Das alte Verhalten ermöglichte uneingeschränkten Port-Zugriff für Shindig-Anfragen, während das neue Verhalten von Administratoren verlangt, explizit zu definieren, auf welche Ports zugegriffen werden kann, um Brute-Force-Angriffe auf offene Ports zu verhindern.

Verwandte Inhalte

- Cisco Bug-ID CSCwt62299
- Finesse-Migrationsdokumentation
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.