# تفشل مكالمات واجهة برمجة التطبيقات الخاصة بالأجهزة (API) FindGet Request الخارجية مع HTTP 400 بعد الترقية إلى PCCE 15.0.1 SU2

## المحتويات

## مسألة

بعد ترقية PCCE 15.0.1 Finesse من SU1 (15.0.1.10100-104) إلى SU2 (15.0.1.10200-61)، فشلت أدوات الطرف الثالث التي تستخدم الأمر Finesse Gadget API MakeRequest لاسترداد سمات الوكيل مع رمز حالة HTTP 400 (طلب سيئ). تعمل نفس وظيفة الأداة الذكية بشكل صحيح عند الرجوع إلى SU1. تمنع هذه المشكلة الأدوات الذكية التابعة لجهات خارجية من إجراء طلبات ناجحة من خلال خدمة الوكيل Finesse Gadget.

تتضمن أعراض الخطأ المحددة ما يلي:

- استجابات HTTP 400 لطلبات POST إلى نقطة نهاية /gadget/makeRequest
- لم تعد تعمل أدوات إعادة البيع التابعة لجهة خارجية
- تم رفض طلبات وكيل أداة المعلومات غير صالحة

## البيئة

- Cisco Packaged Contact Center Enterprise (PCCE)، الإصدار 15.0.1
- تم ترقية Finesse من SU1 (15.0.1.10100-104) إلى SU2 (15.0.1.10200-61)
- وظيفة Finesse Gadget API MakeRequest تستخدم طرف ثالث من ذكية أدوات
- تكوينات نشر PCCE (تم اختبارها بسرعة 2 و 4 آلاف لفة في الدقيقة)

# رارق

سبب هذه المشكلة هو تحسين الأمان الذي تم تقديمه في Finesse 15.0.1 SU2 الذي ينفذ قائمة المنافذ المسموح بها لطلبات العرض (معرف الأخطاء من Cisco CSCwt62299). يتطلب الحل تكوين المنافذ المسموح بها التي يمكن للأدوات الذكية الوصول إليها من خلال واجهة برمجة تطبيقات MakeRequest.

## الخطوة 1: تكوين المنافذ المسموح بها لطلبات العرض

قم بتنفيذ أمر CLI هذا على خادم Finesse لتكوين قائمة المنافذ المسموح بها:

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

يقوم هذا الأمر بتكوين النظام للسماح بطلبات الأدوات الذكية إلى المنافذ المحددة.
تضمين جميع المنافذ التي تحتاج الأدوات الذكية التابعة لجهات خارجية إلى الوصول إليها.

## الخطوة 2: إعادة تشغيل خدمة Tomcat

بعد تكوين المنافذ المسموح بها، قم بإعادة تشغيل خدمة Tomcat لتفعيل التغييرات:

```
utils service restart Cisco Tomcat
```

## الخطوة 3: إعادة تشغيل AW Tomcat (إذا كان ذلك ممكنا)

إذا كانت خدمة AW (بوابة وتطبيق) Tomcat معطلة أو تحتاج إلى إعادة التشغيل، فبادر بتشغيلها أيضا.

## الخطوة 4: التحقق من إعادة تعيين كلمة مرور أداة ذكية لجهة خارجية

تأكد من إعادة تعيين كلمة مرور حساب 3rdpartygadget بعد الترقية، حيث أن هذه مطلوبة Finesse لوظيفة الأداة الذكية من جهة خارجية. يجب إعادة تعيين كلمة المرور على كل من خوادم الأساسية والثانوية إذا كان ذلك ممكنا.

### الخطوة 5: وظيفة الأداة الذكية للاختبار

بعد إكمال تغييرات التكوين وعمليات إعادة تشغيل الخدمة، قم باختبار وظيفة أداة معلومات MakeRequest الآن (API) لتطبيقات واجهة برمجة التطبيقات لتأكيد نجاح إستدعاءات الطرف الثالث دون أخطاء HTTP 400.

## السبب

تم إدخال تحسين أمان يطبق على Finesse 15.0.1 SU2، في Cisco CSCwt62299. تعرف الأخطاء من قائمة مسموح بها من المنافذ لطلبات التجزئة. يمنع هذا التغيير الوصول غير المصرح به إلى منافذ النظام عن طريق طلب تكوين صريح يمكن للأدوات الذكية الخاصة بالمنافذ الوصول إليه من خلال واجهة برمجة تطبيقات MakeRequest. بدون هذا التكوين، يتم حظر جميع طلبات وكيل الأدوات الذكية لعناوين URL الخارجية مع أخطاء HTTP 400 كإجراء أمان ضد هجمات تزوير الطلبات من جانب الخادم (SSRF) المحتملة.

سمح السلوك القديم بالوصول غير المقيد إلى المنفذ لطلبات التجزئة، بينما يتطلب السلوك الجديد من المسؤولين تحديد المنافذ التي يمكن الوصول إليها بشكل صريح لمنع الهجمات العنيفة على المنافذ المفتوحة.

## المحتوى ذي الصلة

- معرفة تصحيح الأخطاء من Cisco CSCwt62299
- وثائق ترحيل Finesse
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).