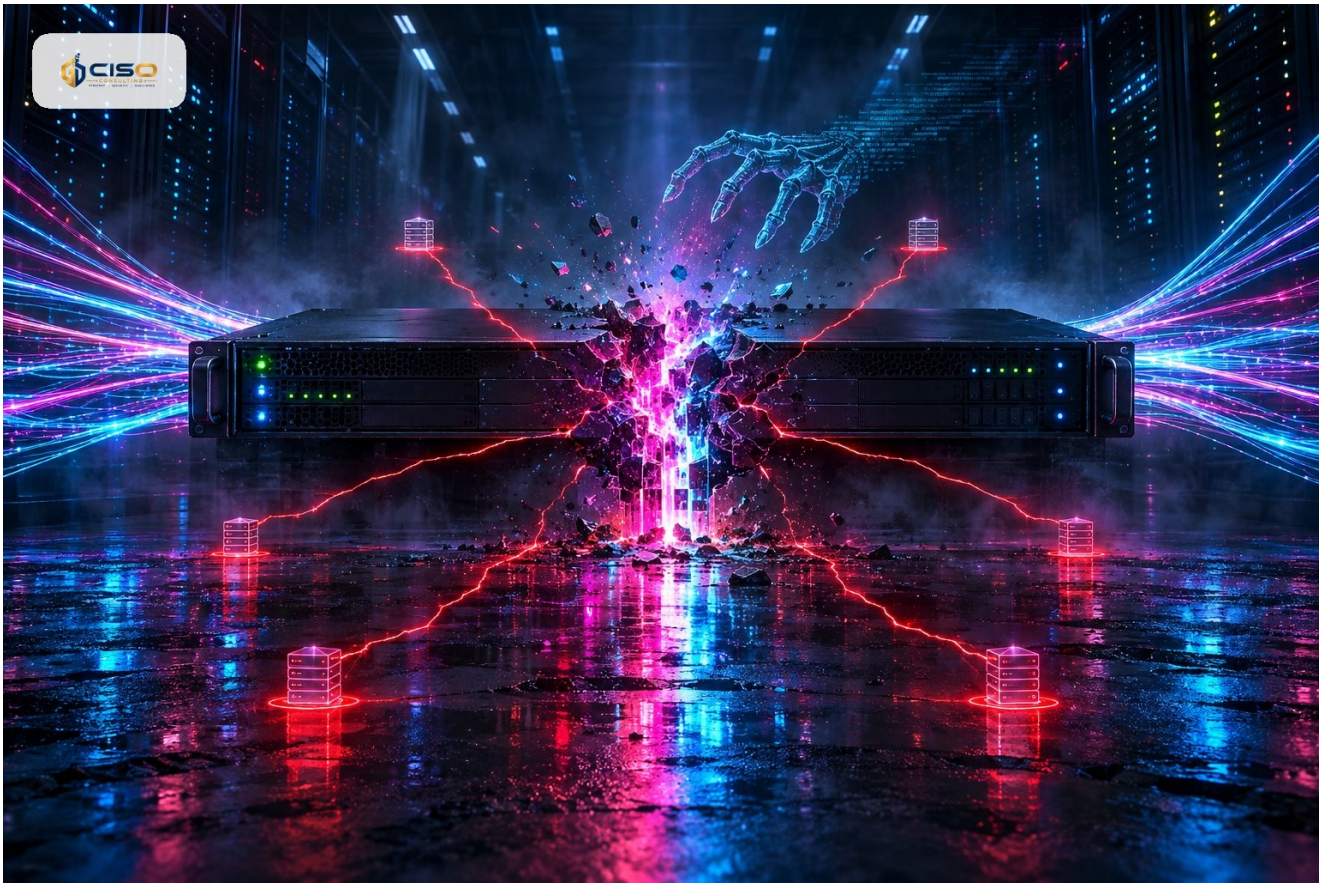
F5 تكشف عن ست ثغرات حرجة في BIG-IP قد تتسبب في تعطل TMM في إعدادات محددة



كشفت F5 عن ست ثغرات حرجة في BIG-IP تتيح لمهاجم دون مصادقة إسقاط TMM وتعطيل حركة البيانات، وتعتمد كل منها على إعداد محدد للخادم الافتراضي. ويشير العنوان كذلك إلى إمكانية تنفيذ أوامر عن بُعد.

- ست ثغرات حرجة تؤثر على BIG-IP من F5.
- يمكن للمهاجم إسقاط TMM (Traffic Management Microkernel) دون تسجيل دخول.
- تتعطل حركة البيانات إلى أن يُعاد تشغيل TMM.
- تتطلب كل ثغرة إعدادًا محددًا للخادم الافتراضي: iRule تستخدم أمرًا معينًا، أو سياسة APM تضم نوعين معينين من الوكلاء.
- يذكر عنوان المصدر أن تنفيذ الأوامر عن بُعد قد يكون ممكنًا.

كشفت F5، الشركة المصنِّعة لمنتج BIG-IP، عن ست ثغرات حرجة في المنتج. ووفق التقرير، يمكن لمهاجم لم يسجّل الدخول استغلالها لإسقاط Traffic Management Microkernel (TMM)، وهو المكوّن المسؤول عن معالجة حركة البيانات، وتبقى الحركة متعطلة إلى أن يُعاد تشغيله.

من المعرّض للخطر

لا تظهر الثغرات في كل عملية نشر، إذ تتطلب كل واحدة منها إعدادًا محددًا على الخادم الافتراضي: إما iRule تستخدم أمرًا معينًا، أو سياسة APM تضم نوعين معينين من الوكلاء. كما يذكر عنوان المصدر أن الثغرات قد تتيح تنفيذ أوامر عن بُعد، لكن المقتطف المتاح لا يورد تفاصيل إضافية عن ذلك.

ما يعنيه ذلك لمنشأتكم

غالبًا ما يقع BIG-IP أمام خدمات أساسية، ولذلك قد يؤدي تعطل TMM إلى انقطاع توافر التطبيقات خلفه. والخطوة العملية الأولى هي التحقق مما إذا كانت الخوادم الافتراضية لديكم تستخدم إعدادات iRule أو APM المتأثرة، فهذا ما يحدد التعرض الفعلي.

ولا يورد المقتطف أرقام CVE ولا الإصدارات المتأثرة ولا الإصلاحات، لذا ينبغي للفرق الرجوع مباشرة إلى نشرة F5 قبل التخطيط لأي تغيير.

ما يجب فعله الآن

1. حصر جميع أجهزة BIG-IP وتحديد الخوادم الافتراضية التي تستخدم iRules أو سياسات APM.
2. مراجعة تلك الـ iRules وسياسات APM وفق شروط الإعداد الواردة في نشرة F5.
3. الحصول على أرقام CVE والإصدارات المتأثرة والإصلاحات من نشرة F5 الرسمية وتخطيط المعالجة بناءً عليها.
4. إعطاء الأولوية للخوادم الافتراضية المواجهة للإنترنت والحيوية للأعمال في المراجعة والترقيع.
5. التأكد من أن مراقبة التوافر والتحويل التلقائي لـ BIG-IP قادران على رصد إعادة تشغيل TMM ومعالجتها، بما يتوافق مع خطط استمرارية الأعمال.