F5 تصدر تصحيحات عاجلة لخمس ثغرات حرجة في BIG-IP



دعت F5 عملاءها إلى تثبيت تصحيحات لخمس ثغرات حرجة في BIG-IP قد يستغلها المهاجمون لتنفيذ هجمات حجب الخدمة أو تنفيذ تعليمات برمجية عن بُعد.

- أصدرت شركة F5 الأمريكية للأمن السيبراني تصحيحات عاجلة لمنتج BIG-IP.
- تشمل التصحيحات خمس ثغرات حرجة.
- قد يؤدي استغلالها إلى حجب الخدمة (DoS) أو تنفيذ تعليمات برمجية عن بُعد (RCE).
- طلبت الشركة من العملاء تثبيت التصحيحات.

حذّرت F5 عملاءها من خمس ثغرات حرجة في BIG-IP، ودعتهم إلى تثبيت التصحيحات. ووفق التقرير، قد يستغل المهاجمون هذه الثغرات لإحداث حالة حجب خدمة أو للحصول على تنفيذ تعليمات برمجية عن بُعد على الأنظمة المتأثرة.

ما الذي يؤكده المصدر

يؤكد النص المتاح عدد الثغرات ودرجة خطورتها ونوعي الأثر المحتمل، وأن F5 أصدرت تصحيحات عاجلة. ولا يتضمن الجزء الذي اطلعنا عليه أرقام CVE ولا الإصدارات المتأثرة ولا إشارة إلى استغلال فعلي، لذا ينبغي الرجوع إلى نشرة F5 الأمنية للحصول على هذه التفاصيل.

أهمية الموضوع

تُنشر أجهزة BIG-IP عادةً على حدود الشبكة وتعالج حركة البيانات لتطبيقات مهمة. وقد يمنح تنفيذ التعليمات عن بُعد على جهاز كهذا المهاجم موطئ قدم قويًا، بينما قد يعطل حجب الخدمة الخدمات المقدمة للعملاء. ولذلك فإن التصحيح في الوقت المناسب مسألة أمنية وكذلك مسألة استمرارية أعمال للجهات المنظمة.

النهج المقترح

تعاملوا مع التحديث كتغيير ذي أولوية: تحققوا من استخدام BIG-IP، واطلعوا على نشرة المورّد لمعرفة الإصدارات المتأثرة، وجدولوا التصحيح عبر مسار التغيير الطارئ مع اختبار وخطة تراجع تناسب أهمية الخدمة.

ما يجب فعله الآن

1. حصر جميع أجهزة BIG-IP وإصدارات برمجياتها في سجل الأصول.
2. مراجعة نشرة F5 الرسمية لتحديد الإصدارات المتأثرة.
3. تثبيت التصحيحات عبر مسار التغيير الطارئ مع إعطاء الأولوية للأجهزة المكشوفة على الإنترنت.
4. حصر الوصول إلى واجهات الإدارة في الشبكات الداخلية الموثوقة.
5. مراقبة سجلات BIG-IP وتوافر الخدمة بحثًا عن أي نشاط غير معتاد بعد التصحيح.