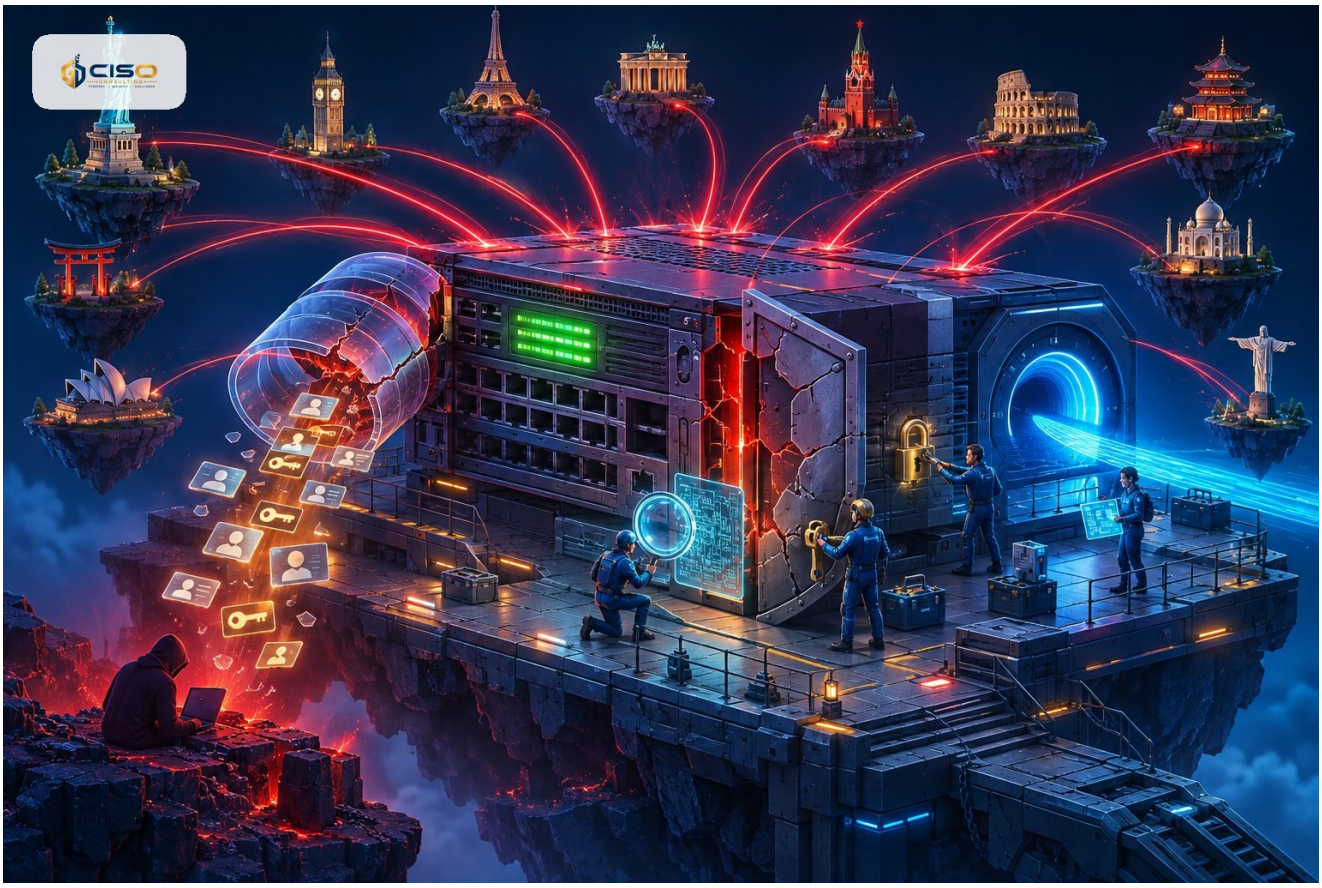
المركز الوطني للأمن السيبراني البريطاني يوصي بإجراءات بعد حملة عالمية تستهدف جدران الحماية وبوابات VPN من Fortinet



يفيد المركز الوطني للأمن السيبراني البريطاني باستهداف عالمي لجدران حماية Fortinet وبوابات VPN، مع تسريب قاعدة بيانات اعتماد. على الجهات التحقق من تعرضها وفحص الأجهزة وتحصينها.

- استُهدفت بوابات FortiGate وVPN المكشوفة على الإنترنت بمحاولات القوة الغاشمة والقواميس وحشو بيانات الاعتماد.
- سرّب طرف تهديد قاعدة بيانات اعتماد، وأشار المركز إلى مؤشرات على أثر محتمل في المملكة المتحدة.
- يمكن استخدام أداتي FortiBleed من SOCRadar وHudson Rock لفحص النطاقات.
- عند ثبوت الاختراق يجب عزل الجهاز وإعادة ضبط المصنع، لأن تغيير كلمات المرور وحده قد لا يزيل الاستمرارية.

- يشمل التحصين المصادقة متعددة العوامل لكل دخول إلى VPN والإدارة، وعدم كشف واجهات الإدارة، والتحديث.

أصدر المركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC) تنبيهاً بشأن حملة عالمية تستهدف جدران الحماية وبوابات VPN من Fortinet، مع مؤشرات على أثر محتمل في بريطانيا. والإرشادات موجهة للجهات البريطانية، غير أن توصياتها التقنية تنطبق على أي جهة تشغّل هذه الأجهزة.

ما الذي حدث

سرّب طرف تهديد قاعدة بيانات اعتماد جُمعت عبر محاولات القوة الغاشمة والقواميس و**حشو بيانات الاعتماد** (credential stuffing) ضد بوابات FortiGate وVPN المكشوفة على الإنترنت. ويعتمد حشو بيانات الاعتماد على إعادة استخدام كلمات مرور مسروقة من خدمة في خدمات أخرى.

ما يوصي به المركز

على الجهات التي تستخدم أجهزة Fortinet الطرفية، وخاصة مع تفعيل SSL VPN، أن تفحص أي نشاط خبيث وأن تراقب الشبكة بحثاً عن سلوك غير معتاد. وأولوياتها:

- فحص النطاقات بأداتي FortiBleed من SOCRadar أو Hudson Rock والتأكد من أن الجهاز يعود للجهة.
- البحث عن مؤشرات الاختراق، ومنها إنشاء حسابات غير مصرح بها ونشاط غير متوقع في السجلات.
- عزل الجهاز عن الإنترنت وعن الشبكة الداخلية عند ثبوت الاختراق.
- حفظ السجلات والإعدادات والأدلة الأخرى ثم إعادة ضبط المصنع، فتغيير كلمات المرور وحده قد لا يكفي.
- فحص الأجهزة الطرفية التي تشترك في بيانات الاعتماد نفسها والأجهزة التي يمكن الوصول إليها من الجهاز المتأثر.

وعند إعادة التشغيل ينصح المركز بعدم كشف واجهات الإدارة على الإنترنت، والتحديث إلى أحدث إصدار، وإزالة الأنظمة غير المدعومة، واستبدال كلمات مرور المسؤولين الافتراضية أو المعاد استخدامها، وفرض المصادقة متعددة العوامل على دخول VPN والإدارة، وتفعيل PBKDF2 لحسابات المسؤولين.

كما نشرت Fortinet مقالًا يتضمن إرشادات وتحليلًا.

ما يجب فعله الآن

1. حصر جميع جدران حماية Fortinet وبوابات VPN وتحديد المكشوف منها على الإنترنت مع تفعيل SSL VPN.
2. فحص نطاقات الجهة بأداتي FortiBleed من SOCRadar وHudson Rock ومراجعة إرشادات Fortinet المنشورة.
3. مراجعة سجلات الأجهزة والحسابات بحثاً عن مؤشرات الاختراق مثل حسابات مسؤول غير مصرح بها.
4. عند اختراق أي جهاز: حفظ الأدلة وعزله وإعادة ضبط المصنع وفحص الأجهزة التي تشترك في بيانات

اعتماده أو يمكن الوصول إليها منه.

5. فرض المصادقة متعددة العوامل على كل دخول إلى VPN والإدارة، وإغلاق كشف واجهات الإدارة، واستبدال كلمات المرور الافتراضية أو المعاد استخدامها، وتحديث البرمجيات.
6. إبلاغ الهيئة الوطنية للأمن السيبراني والجهة التنظيمية القطاعية عن الحوادث المؤكدة وفق المتطلبات المعمول بها.