

بريطانيا و12 دولة حليفة تصدر تنبيهاً بشأن استهداف FSB الروسي لأجهزة التوجيه في البنى التحتية الحرجة



أصدر المركز الوطني للأمن السيبراني البريطاني و18 جهة من 12 دولة تنبيهاً مشتركاً يحذر من استغلال المركز 16 التابع لجهاز الأمن الفيدرالي الروسي لأجهزة التوجيه ضعيفة الإعداد لاستهداف البنى التحتية الحرجة عالمياً.

- المركز 16 التابع لجهاز الأمن الفيدرالي الروسي يفحص الإنترنت بحثاً عن أجهزة توجيه تستخدم كلمات مرور SNMP افتراضية أو ضعيفة ويستغل ثغرات معروفة في أجهزة Cisco
- قطاعات الاتصالات والدفاع والطاقة والخدمات المالية والحكومة والرعاية الصحية تواجه أعلى مستوى من المخاطر من هذه الحملة الاستهدافية العالمية
- التنبيه المشترك من 19 جهة عبر 13 دولة يوصي بالانتقال إلى SNMPv3 وتطبيق كلمات مرور قوية فريدة وتقييد الوصول إلى بروتوكولات الإدارة
- التحذير يتزامن مع عقوبات بريطانية ضد 24 كياناً وإسناد رسمي لهجوم ديسمبر 2025 على شبكة

الطاقة البولندية إلى المركز 16 التابع لجهاز الأمن الفيدرالي

• يُحث المؤسسات على الحصول على شهادة Cyber Essentials واستخدام إطار التقييم السيرياني المحدث لتقييم النضج الأمني

أصدر المركز الوطني للأمن السيرياني البريطاني بالتعاون مع 18 جهة شريكة من أستراليا وكندا والجمهورية التشيكية والدنمارك وإستونيا وفنلندا وفرنسا وإيطاليا ونيوزيلندا وبولندا والسويد والولايات المتحدة تنبهاً سيريانياً مشتركاً يحذر من استغلال نشط للبنية التحتية الشبكية من قبل جهات فاعلة تابعة للدولة الروسية.

أساليب الجهة المهددة

يحدد التنبيه المركز 16 التابع لجهاز الأمن الفيدرالي، المعروف أيضاً باسم Energetic Bear و Berserk Bear و Static Tundra و Ghost Blizzard و Dragonfly و Crouching Yeti كجهة تقوم بفحص انتهازي لأجهزة التوجيه المتصلة بالإنترنت لتحديد الأجهزة المهيأة بكلمات مرور افتراضية أو ضعيفة لبروتوكول إدارة الشبكة البسيط وسلاسل المجتمع. كما استغلت الجهة المهددة ثغرات معروفة في أجهزة Cisco وميزة Smart Install و عيوب البوابات الإلكترونية للسيطرة على معدات الشبكة.

الاستهداف عالمي النطاق ويركز على المؤسسات العاملة في قطاعات الاتصالات والدفاع والطاقة والخدمات المالية والحكومة والرعاية الصحية. أسندت بريطانيا ودول الاتحاد الأوروبي رسمياً هجوماً وقع في ديسمبر 2025 على شبكة الطاقة البولندية إلى هذه الجهة، مشيرة إلى أن الهجوم كان من الممكن أن يعطل إمدادات الكهرباء لـ 500,000 مدني.

الضوابط الفنية الموصى بها

يوصي التنبيه المؤسسات بالانتقال إلى SNMPv3 وتعطيل إصدارات SNMP القديمة، وتطبيق كلمات مرور قوية وفريدة لجميع أجهزة الشبكة، وتقييد الوصول إلى بروتوكولات الإدارة من خلال ضوابط وصول مناسبة. كما يشجع المركز الوطني للأمن السيرياني المؤسسات على الحصول على شهادة Cyber Essentials واستخدام إطار التقييم السيرياني المحدث لتقييم النضج الأمني ومعالجة الثغرات.

يرافق الإفصاح المنسق عقوبات حكومية بريطانية ضد 24 فرداً وكياناً متورطين في عمليات سيريانية وهجينة مدمرة مرتبطة بأجهزة الاستخبارات الروسية.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع أجهزة التوجيه والأجهزة الشبكية المتصلة بالإنترنت لتحديد المعدات التي تستخدم إعدادات SNMP افتراضية أو ضعيفة
2. الانتقال ببروتوكولات إدارة الشبكة إلى SNMPv3 وتعطيل SNMPv1 و SNMPv2c على جميع أجهزة البنية التحتية
3. تطبيق كلمات مرور قوية وفريدة لجميع حسابات الإدارة لأجهزة الشبكة وتغيير سلاسل المجتمع الافتراضية
4. مراجعة وتقييد الوصول إلى بروتوكولات الإدارة (SSH و Telnet) من خلال تقسيم الشبكة وقوائم التحكم بالوصول

5. مراجعة أجهزة Cisco للكشف عن الثغرات المعروفة وتعطيل ميزة Smart Install حيثما لا تكون مطلوبة وتطبيق تصحيحات الأمان من الموزد

6. تقييم الوضع الأمني الحالي مقابل إطار التقييم السيبراني للمركز الوطني للأمن السيبراني البريطاني والنظر في الحصول على شهادة Cyber Essentials للضوابط الأساسية