تقرير InfraTrust: أجهزة الشبكات معرّضة للخطر عبر ثغرات PHP2Shell



يفيد تقرير InfraTrust بأن مهاجمين يستغلون ثغرات في البنية التحتية الحرجة للشبكات، وأن ثغرات PHP المسماة PHP2Shell تعرّض واجهات الإدارة عبر الويب لجدران الحماية وشبكات VPN وأجهزة مشابهة للخطر.

- يفيد InfraTrust بوجود استغلال فعلي لثغرات في البنية التحتية الحرجة للشبكات.
- تُعرف ثغرات PHP المعنية باسم PHP2Shell.
- تشمل الفئات المتأثرة جدران الحماية وشبكات VPN ووحدات توصيل التطبيقات.
- يتركز الخطر في واجهات الإدارة عبر الويب لهذه الأجهزة.
- لا يتضمن المقتطف المتاح أي تفاصيل عن الموردين أو أرقام CVE أو التحديثات.

ما الذي ورد في التقرير

يحذّر تقرير صادر عن InfraTrust، نقله موقع BleepingComputer، من أن مهاجمين يستغلون فعليًا ثغرات في البنية التحتية الحرجة للشبكات. ويسلّط الضوء على مجموعة ثغرات في PHP تُعرف باسم **PHP2Shell**، تعرّض واجهات الإدارة عبر الويب لأجهزة الشبكات للخطر.

ومن أنواع الأجهزة المذكورة جدران الحماية وشبكات VPN ووحدات توصيل التطبيقات، إضافة إلى أجهزة مشابهة. وتقع هذه الأجهزة عادةً عند حدود الشبكة وتمتلك صلاحيات مرتفعة، لذا فإن أي ضعف في طبقة إدارتها يستحق الاهتمام.

ما لا نعرفه حتى الآن

لا يذكر المقتطف المتاح الموردين أو المنتجات المتأثرة، ولا أرقام CVE أو درجات الخطورة أو الإصلاحات. لذلك ينبغي ألا تفترض المؤسسات أن جهازًا بعينه متأثر أو غير متأثر، وأن تتحقق مباشرة من مورديها.

قراءة عملية للجهات في المملكة

القاسم المشترك هو انكشاف واجهات الإدارة. ويُعد تقليص من يستطيع الوصول إليها والتأكد من حالة كل جهاز استجابة معقولة ريثما تتضح التفاصيل. كما يُنصح بمراجعة التقرير الأصلي عند توفر نصه الكامل.

ما يجب فعله الآن

1. حصر جدران الحماية وشبكات VPN ووحدات توصيل التطبيقات وتحديد ما يتيح منها واجهة إدارة عبر الويب.
2. قصر الوصول إلى واجهات الإدارة على شبكات داخلية مخصصة أو أجهزة إدارية، وعدم إتاحتها عبر الإنترنت.
3. سؤال موردي الأجهزة عمّا إذا كانت منتجاتهم متأثرة بـ PHP2Shell وتطبيق أي إصلاحات تصدر.
4. مراجعة سجلات الأجهزة والإدارة بحثًا عن وصول غير متوقع أو تغييرات في الإعدادات.
5. تسجيل المسألة في سجلات إدارة الثغرات ومخاطر الأطراف الثالثة ضمن عمليات ضوابط NCA ECC وإطار SAMA CSF.