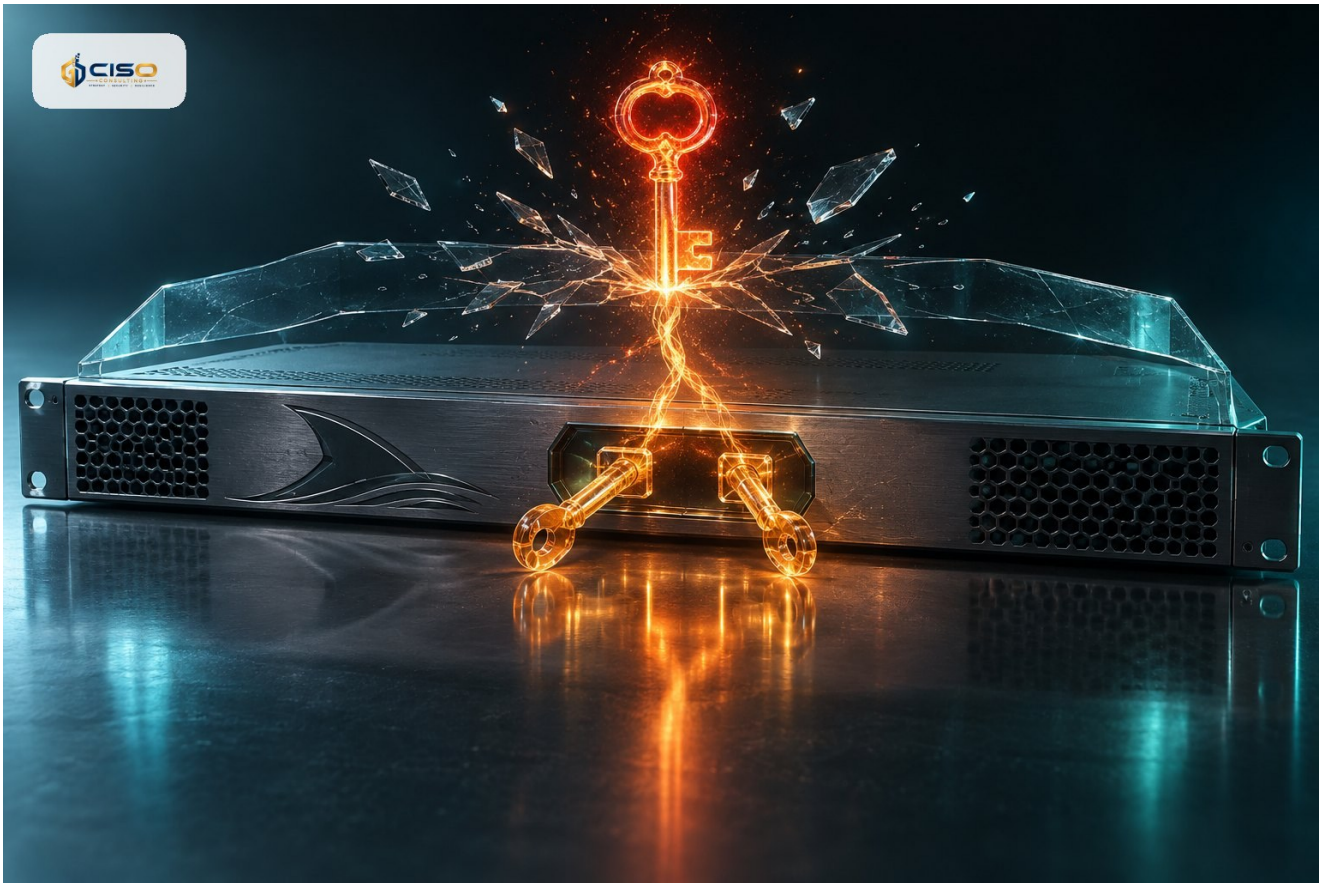
Barracuda تصدر تحديثات لثغرتين قد تتيحان الوصول بصلاحيات الجذر إلى أجهزتها



أصدرت Barracuda تحديثات للثغرتين CVE-2026-116606 وCVE-2026-111560 اللتين قد تتيحان معًا لمهاجم يصل إلى واجهة الإدارة الحصول على صلاحيات الجذر. يُنصح بتحديث البرامج الثابتة وتقييد الوصول الإداري.

- الثغرة CVE-2026-116606 حرجة، وهي ضعف في المصادقة بجهاز Email Security Gateway يتيح تعديل الإعدادات العامة للجهاز.
- الثغرة CVE-2026-111560 تتيح لمن يملك صلاحيات إدارية حقن أوامر نظام تشغيل تُنفَّذ بصلاحيات الجذر.
- يتطلب الاستغلال الوصول إلى واجهة الإدارة؛ وعند الجمع بين الثغرتين قد يُتجاوز التفويض ويُنال وصول الجذر.
- تشمل المنتجات المتأثرة أيضًا WAF Controlg Message Archiverg Load Balancer ADC

Web Security Gateway و Web Application Firewall و Center.

- سبق أن استُهدفت أجهزة Barracuda ESG في هجمات يوم الصفر عام 2023.

طلبت Barracuda Networks من عملائها تطبيق تحديثات لثغرتين قد تسمحان بتنفيذ أوامر بصلاحيات الجذر على أجهزتها.

ما تتيحه الثغرتان

الأولى **CVE-2026-116606** مصنفة حرجة، وتنشأ من ضعف في المصادقة بجهاز (ESG Email Security Gateway) يمكن للمهاجم استغلاله لتعديل الإعدادات العامة للجهاز. أما الثانية **CVE-2026-111560** فتتيح لمهاجم يملك صلاحيات إدارية حقن أوامر نظام تشغيل تُنفَّذ بصلاحيات الجذر.

وتوضح Barracuda أن الاستغلال يتطلب الوصول إلى واجهة الإدارة للمنتج المستهدف. وإذا استُخدمت الثغرتان معًا فقد يتجاوز المهاجم ضوابط التفويض ويحصل على وصول الجذر إلى الجهاز.

المنتجات المتأثرة والإصلاحات

إضافةً إلى ESG، تشمل قائمة الشركة ADC Load Balancer و(BMA Message Archiver) و(WCC WAF Control Center) و(WAF Web Application Firewall) و(WSG Web Security Gateway). وتُعرَّف التحديثات بمراجع مثل BNSF-40425 للإصدار 9.4.017 وما بعده من ESG، وBNSF-40430 للإصدارات الأقدم. وتدعو الشركة العملاء إلى مراجعة إرشادات المعالجة، وتشغيل أحدث إصدار من البرنامج الثابت، وتطبيق جميع التحديثات الأمنية، مع ضوابط وصول شبكية تحصر الوصول الإداري في الشبكات الداخلية الموثوقة.

السياق

سبق أن استُهدفت أجهزة ESG؛ فقد أصلحت Barracuda الثغرة CVE-2023-7102 بعد استغلالها من مجموعة UNC4841 كثغرة يوم صفر، واستغلت المجموعة نفسها الثغرة CVE-2023-2868 في هجمات تجسس طالت، بحسب Mandiant، جهات حكومية بنسبة كبيرة. ولا يذكر المصدر استغلالاً للثغرتين الجديدتين.

ما يجب فعله الآن

1. حصر جميع أجهزة Barracuda من نوع ESG وADC وBMA وWCC وWAF وWSG والتأكد من إصدارات البرامج الثابتة.
2. تطبيق التحديثات الموردة لكل منتج متأثر مع إعطاء الأولوية لـ Email Security Gateway.
3. حصر واجهات الإدارة في الشبكات الداخلية الموثوقة ومنع الوصول إليها من الإنترنت أو من شرائح المستخدمين العامة.
4. مراجعة الحسابات الإدارية والتغييرات الأخيرة في الإعدادات على هذه الأجهزة بحثًا عن أي نشاط غير متوقع.
5. توثيق عملية التحديث ضمن إدارة الثغرات بما يتوافق مع متطلبات ضوابط NCA ECC وإطار SAMA CSF.