اختراق لدى Radware يكشف بيانات اعتماد تصدير سجلات Cloud WAF لبعض العملاء



أفادت Radware بأن واجهة إدارة داخلية لخدمة Cloud WAF كانت متاحة عبر الإنترنت دون مصادقة، فكُشفت بيانات اتصال العملاء وبيانات اعتماد تصدير السجلات لدى بعضهم. يُنصح العملاء المتأثرون بتدوير المفاتيح.

- في 19 نوفمبر 2026 وصلت جهة غير مصرح لها إلى واجهة إدارة داخلية لخدمة Cloud WAF كانت متاحة عبر الإنترنت دون مصادقة.
- البيانات المحتمل الوصول إليها: بيانات اتصال العملاء، ولدى بعضهم بيانات اعتماد تصدير السجلات إلى AWS S3 أو Azure Blob Storage أو SFTP.
- تذكر Radware أنه لم يُرصد كشف لفحص حركة WAF أو الشهادات أو بيانات المستخدمين النهائيين أو حركة التطبيقات أو خدمات الحماية من DDoS السحابية.
- أبلغ بعض العملاء عن تنبيهات في AWS بشأن عنوان IP غير مألوف يحاول الوصول إلى حاويات

تصدير السجلات، والتحقيق مستمر.

- توصي Radware بشدة العملاء المتأثرين في AppSec (WAF وBOT) بتدوير بيانات الاعتماد ومراجعة سجلات الوصول للتخزين منذ 19 نوفمبر على الأقل.

كشفت Radware أن مهاجمين وصلوا إلى واجهة إدارة داخلية لخدمة Cloud WAF كانت مكشوفة على الإنترنت دون اشتراط مصادقة. وبحسب تقرير تحليل السبب الجذري الذي نقلته BleepingComputer، وقع الوصول غير المصرح به في 19 نوفمبر 2026 واكتُشف بعد نحو عشر ساعات.

ما الذي انكشف

تذكر الشركة أن المعلومات التي ربما جرى الوصول إليها تشمل بيانات الاتصال بالعملاء، وبالنسبة لعدد منهم بيانات الاعتماد المهيأة لتصدير السجلات إلى تخزين يديره العميل بنفسه: AWS S3 أو Azure Blob Storage أو SFTP. وتؤكد أن فحص حركة WAF والشهادات وبيانات المستخدمين النهائيين وحركة تطبيقات العملاء وخدمات DDoS السحابية وبياناتها لم تتعرض للكشف، وأنها لم تجد دليلًا على تغيير سياسات الأمن لدى العملاء.

ما زال التحقيق جارياً، إذ تعمل Radware على تحديد ما إذا استُخدمت المفاتيح المكشوفة دون إذن. وقد أبلغ بعض العملاء بالفعل عن تنبيهات في AWS بشأن عنوان IP غير مألوف يحاول الوصول إلى حاويات تصدير السجلات.

الإجراءات حتى الآن

حجبت Radware عنوان IP المصدر والوصول إلى الواجهة، وألغت جميع بيانات الاعتماد الداخلية واستبدلتها. وتنصح بشدة عملاء AppSec (WAF وBOT) المتأثرين بتدوير بيانات اعتماد تصدير سجلات Cloud WAF في أقرب وقت، ومراجعة سجلات الوصول للتخزين بحثاً عن نشاط غير متوقع منذ 19 نوفمبر على الأقل. ولم تكن الشركة قد أصدرت بياناً علنياً وقت نشر التقرير.

أهمية الخبر

تمنح بيانات اعتماد تصدير السجلات وصولًا إلى تخزين قد يحتوي على سجلات الطلبات. وعلى الجهات التي تستخدم Cloud WAF مع تخزين خاص بها اعتبار هذه المفاتيح مكشوفة محتملًا إلى أن يثبت العكس، والتحقق من وجود التزامات تعاقدية للإبلاغ.

ما يجب فعله الآن

1. تحقق مما إذا كانت جهتكم تستخدم Radware Cloud WAF مع تصدير السجلات إلى AWS S3 أو Azure Blob Storage أو SFTP، وتواصلوا مع Radware لمعرفة ما إذا كنتم من المتأثرين.
2. دوّروا بيانات اعتماد تصدير السجلات فوراً: مفاتيح AWS ومفاتيح تخزين Azure أو رموز SAS وبيانات SFTP.
3. راجعوا سجلات الوصول لحسابات تخزين السجلات المصدّرة منذ 19 نوفمبر 2026 بحثاً عن عناوين IP غير مألوفة أو قراءات غير متوقعة.
4. قيّدوا الوصول إلى تخزين السجلات المصدّرة بأقل الصلاحيات وبقوائم سماح لعناوين IP المصدر حيثما أمكن.

5. عند اكتشاف وصول غير مصرح به، فعّلوا خطة الاستجابة للحوادث وقيّموا التزامات الإبلاغ للهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي (ساما) أو سدايا وفق المتطلبات والعقود المعمول بها.
6. أدرجوا سيناريوهات كشف بيانات الاعتماد لدى الأطراف الثالثة في مراجعات مخاطر الموردين.