شركة SAP تعالج أربع ثغرات بأقصى درجات الخطورة في Web Dispatcherg NetWeaver



عالجت SAP في يوم التحديثات الشهري أربع ثغرات بدرجة CVSS 10.0 يمكن استغلالها دون تسجيل دخول، ثلاث منها في خادم تطبيقات NetWeaver وواحدة في Web Dispatcher.

- أصلحت SAP أربع ثغرات في يوم التحديثات الأمنية الشهري، وصُنّفت كل منها بدرجة 10.0 وهي الحد الأقصى في CVSS.
- يمكن للمهاجمين استغلال الثغرات الأربع دون مصادقة.
- ثلاث ثغرات في خادم تطبيقات SAP NetWeaver، وهو البرنامج الذي تعمل عليه أنظمة SAP.
- ثغرة واحدة في Web Dispatcher الذي يستقبل طلبات الويب من الإنترنت ويمررها إلى خادم التطبيقات.
- يشير عنوان الخبر إلى أن ثغرتين منها تتيحان تنفيذ تعليمات برمجية عن بُعد.

أصدرت SAP تحديثات يوم التحديثات الأمنية الشهري، وعالجت أربع ثغرات صنّفتها بدرجة 10.0، وهي أعلى درجة ممكنة في CVSS. ووفق التقرير، يمكن للمهاجمين استغلال الثغرات الأربع دون تسجيل دخول.

ما الذي تأثر

ثلاث من الثغرات في خادم تطبيقات SAP NetWeaver، وهو البرنامج الذي تعمل عليه أنظمة SAP. أما الرابعة ففي Web Dispatcher، المكوّن الذي يستقبل طلبات الويب من الإنترنت ويمررها إلى ذلك الخادم. ويشير عنوان التقرير إلى أن ثغرتين من الأربع تتيحان تنفيذ تعليمات برمجية عن بُعد.

لا يتضمن المقتطف المتاح لنا أرقام CVE ولا الإصدارات المتأثرة ولا أي دليل على استغلال فعلي، ولذلك ينبغي الرجوع إلى ملاحظات SAP الأمنية الرسمية لهذه التفاصيل.

أهمية الأمر

لأن الثغرات لا تتطلب مصادقة، ولأن Web Dispatcher يقع عند النقطة التي تصل منها حركة الإنترنت إلى بيئات SAP، فإن الأنظمة المكشوفة على الإنترنت هي الأكثر عرضة للخطر. وعلى الجهات التي تشغّل SAP للشؤون المالية أو المشتريات أو الموارد البشرية أن تعامل هذا الإصدار بأولوية، وألا تنتظر دورة التحديثات المعتادة.

الخطوة التالية

حدّدوا نسخ NetWeaver وWeb Dispatcher لديكم، وراجعوا ملاحظات SAP للإصدارات المتأثرة، وجدولوا الإصلاحات عبر مسار التغيير الطارئ، بدءًا بالأنظمة المكشوفة على الإنترنت.

ما يجب فعله الآن

1. احصروا جميع نسخ خادم تطبيقات SAP NetWeaver وWeb Dispatcher، مع تحديد ما يمكن الوصول إليه من الإنترنت.
2. راجعوا ملاحظات SAP الأمنية الرسمية لهذا الإصدار لتحديد الإصدارات المتأثرة والإصلاحات الخاصة بالثغرات الأربع بدرجة CVSS 10.0.
3. طبّقوا التحديثات عبر مسار التغيير الطارئ، بدءًا بالأنظمة المكشوفة على الإنترنت.
4. إذا تعذّر التحديث فورًا، فقيّدوا الوصول إلى Web Dispatcher وراقبوه عن كثب بحثًا عن طلبات غير معتادة.
5. وثّقوا التقييم والمعالجة لإثبات إدارة الثغرات وفق ضوابط الهيئة الوطنية للأمن السيبراني (NCA ECC) وإطار الأمن السيبراني للبنك المركزي السعودي (SAMA CSF).