

في مارس سنومكس 2017nd ، ثغرة في تطبيق ويب المسمى Apache Tomcat Struts 2 تم اكتشافه بواسطة باحث أمني وتم تحديده على أنه ضعف CVE-2017-5638 تم استخدام تطبيق الويب هذا بواسطة Equifax للسماح للمستهلكين بتقديم تناقضات في تقرير الانتماء. بعد أيام من اكتشاف الثغرة الأمنية ، تم إتاحة تصحيح البرنامج في 7 مارس 2017 ونشره للعامة. في غضون 24 ساعة من التصحيح ، ظهر منشور مدونة على موقع ويب حول كيفية استغلال هذه الثغرة الأمنية للوصول عن بُعد إلى أجهزة الكمبيوتر التي تشغل البرنامج غير المصحح. في 10 مارسth في عام 2017 ، تم إصدار الاستغلال كمكوّن إضافي لمجموعة أدوات استغلال المصدر المفتوح الشهيرة المسماة Metasploit وبدأ المتسللون في استخدام هذه الأداة لفحص الإنترنت بحثًا عن الخوادم التي بها هذه الثغرة الأمنية. في وقت ما في منتصف شهر مايو من عام 2017 ، تلقى المتسللون ضربة وصادف أن الخادم ينتمي إلى Equifax. تم الحصول على وصول غير مصرح به وظل المتسللون داخل شبكة Equifax ، وقاموا بسحب البيانات حتى تم اكتشافهم في 29 يوليوth، 2017.

لماذا حدث الخرق؟

قد يعتقد المرء أن مؤسسة بحجم Equifax ومسؤولة عن حماية بيانات 145 مليون أمريكي ، كانت قادرة على اكتشاف هذا الانتهاك قبل سرقة البيانات ، ناهيك عن كونها غير برامج لمدة 2.5 شهرًا. إذا ماذا حصل؟ وفقًا للتقارير ، تم إبلاغ Equifax بالثغرة الأمنية ، ومع ذلك لم يتخذ أي إجراء لتصحيح الخادم. بمجرد عدم إصلاح الخادم وبدأ المتسللون في استغلال الثغرة الأمنية ، انطلقت "التنبيهات المشبوهة" ولكن Equifax لم تتخذ أي إجراء. لإعادة صياغة الرئيس التنفيذي السابق لـ Equifax ، فإنهم يتلقون آلاف التنبيهات كل عام ومن الصعب تحديد التنبيهات المهمة من التنبيهات غير المهمة. هذا يسلط الضوء بوضوح على مشكلة أدوات الأمان ومشكلة الأشخاص. تواجه الأدوات التي تنشرها المؤسسات اليوم وقتًا عصيبًا في تحديد الأحداث الحرجة من الأحداث غير الحرجة ، وسيكون هناك دائمًا خطأ بشري ولن يكون هناك عدد كافٍ من الأشخاص للاستجابة للتهديدات.

ما الذي كان يمكن فعله؟

بالنسبة للمبتدئين ، كان من الممكن تجنب الخطأ البشري إذا كان Equifax قد اهتم بنشرة الثغرات الأمنية المسمى CVE-2017-5638 وقام بتصحيح خوادمهم بسرعة. ثانيًا ، تحتاج المؤسسات إلى البدء في إنهاء صلاحية الأدوات القديمة التي تمنح المؤسسات إحساسًا زائفًا بالأمان للمنظمات الجديدة التي تعالج مشكلة العصر الحديث. ستؤدي أدوات مثل أنظمة كشف التسلل (IDS) ومعلومات الأمان ومديري الأحداث (SIEM) وصندوق الحماية من البرامج الضارة التي تعمل بشكل مستقل عن بعضها البعض

وتوضع بشكل غير منتشر داخل البنية التحتية إلى تنبيه ضوضاء ونقاط عمياء وقدرة محدودة على الاكتشاف. مع أنظمة IDS ، تم تصميمها بشكل كبير حول الاكتشاف القائم على التوقع ، مما يعني أنها تستطيع اكتشاف الهجمات المعروفة. أنظمة IDS غير كافية لاكتشاف ثغرات Zero-Day ، حيث لا يوجد توقع متاح لطريقة هجوم جديدة. أصبحت أدوات SIEM أماكن إغراق للسجلات والسجلات والمزيد من السجلات. على الرغم من أن أدوات SIEM هذه مفيدة إلا أنه يجب برمجتها لتشغيل الاستعلامات للبحث عن الأشياء التي تريد البحث عنها. لكن مرة أخرى ، ماذا عن الأشياء الخبيثة المجهولة التي تريد البحث عنها.

إحدى الطرق التي كان من الممكن اتباعها ، هي أن يكون لديك إطار رؤية منتشر على نطاق واسع في جميع أنحاء البنية التحتية Equifax للتخلص من النقاط العمياء ، وجمع أنواع متعددة من بيانات البنية التحتية ، ثم تشغيل خوارزميات التعلم الآلي أعلى مجموعة البيانات لاكتشاف التشوهات. يطلق على هذه الأطر الجديدة أنظمة الكشف عن الخرق ويتم بناؤها حول تقنية البيانات الضخمة والذكاء الاصطناعي.

ملاحظات ختامية

ما تعلمناه جميعًا في مجال الأمن السيبراني هو أن اختراق البيانات أمر لا مفر منه ، والشبكات في حالة تغير دائم ، ولن تكون هناك حماية بنسبة 100٪ ، وسنشهد كل عام زيادة في الهجمات الإلكترونية. في ضوء ذلك ، تحتاج المؤسسات إلى البحث باستمرار عن طرق جديدة لحماية بياناتها القيمة. في Stellar Cyber ، نعتقد أن أدوات الكشف عن الاختراق المستخدمة اليوم ، مثل IDS و APT و SIEM ، ستتحول وتبدو مختلفة جذريًا في المستقبل القريب.