NTRA
National Telecom Regulatory Authority
الجـــهاز القـــومي لتنـــظيم الإتصـالات

EG|CERT

تحـــذير أمـــني

حرج | عالي | متوسط | منخفض

اسم المنشأه	TREND MICRO™
الجمهور المستهدف	قطاع المؤسسات
التفاصيل	الاصدار المتأثر

الشرح

أصدرت شركة ترينـد مايكرو العالمية الرائدة في مجال حلول الأمن الرقمي نشرتها الأمنية لحزم تحديثات الأنظمة والتطبيقات لحلولها في مجال أمن النقاط الطرفية «ترينـد مايكرو ابيكس ون Trend Micro «Apex One، و «أبيكس ون»(Apex One) .

اللغة	منصة الاستخدام	الاصدار المتأثر	المنتج
	ويندوز	البرنامج المثبت على أجهزة المؤسسة أو الشركة - ٢٠١٩	ابيكس وان
	ويندوز	Saas	

الحلول المقدمة

المنتج	النسخة المحدثة	ملحوظة	منصة الاستخدام	الاتاحة
ابيكس ون (البرنامج يتم تثبيته على الأجهزة الموجودة بالمؤسسة)	CP 8400	ملف Readme	ويندوز	متاح حاليًا
ابيكس ون (البرمجيات كخدمة (SaaS))	حزمة التحديثات الشهرية (سبتمبر 2020)	ملف Readme	ويندوز	متاح حاليًا

الحلول المقدمة

- ثغرة تجاهل المصادقة (CVE-٢٠٢٠-٢٤٥٦٣): قد تسمح هذه الثغرة الأمنية للمهاجم باستغلال خاصية تعطيل security agent (إذا تم ضبط الاعدادات الخاصة بذلك) ، وبالتالي يمكنه تنفيذ التعليمات البرمجية والقيام بالهجوم.
- ثغرة أمنية تَمكن المهاجم من اختراق كافة البيانات الهامة والحساسة (CVE-٢٠٢٠-٢٤٥٦٤, CVE-٢٠٢٠-٢٤٥٦٥, CVE-٢٠٢٠-٢٥٧٧٠, CVE-٢٠٢٠-٢٥٧٧١, CVE-٢٠٢٠-٢٥٧٧٢).
- ثغرة (CVE-٢٠٢٠-٢٥٧٧٣): هذه الثغرة الامنية تُمكن المهاجم من تنفيذ تعليمات برمجية عشوائية على المنتجات المتأثرة.
- ثغرة (CVE-٢٠٢٠-٢٥٧٧٤): تُمكن هذه الثغرة الأمنية المهاجم من الوصول إلى معلومات حساسة لا يُسمح للكثيرين بالوصول لها.

التوصيات

- يتطلب استغلال هذا النوع من الثغرات الأمنية أن يكون للمهاجم قادرًا على الوصول إلى جهاز غير مؤمن. يُنصح العملاء باستخدام التحديثات والحلول المحدثة في التوقيتات المحددة لها، كما يُنصحوا أيضًا بمراجعة خاصية الوصول عن بُعد للأنظمة الهامة والتأكد من تحديث السياسات وتأمين الأجهزة والشبكات.
- قد تحمي الإصدارات الأحدث لأنظمة التشغيل (مثل Windows ١٠) من بعض الثغرات الأمنية مثل hard link privilege escalations.

تاريخ التحذير	١٣/١٠/٢٠٢٠

وعلى الرغم من أن استغلال الثغرات الأمنية قد يتطلب توفر عدة شروط محددة ، فإن المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات EG|CERT يهيب بالمستخدمين القيام بعمل التحديثات اللازمة في أقرب وقت ممكن من خلال الرابط التالي :
https://success.trendmicro.com/solution/000271974