ميلتداون وسبيكتر، أخطر ثغرات المعالجات على الإطلاق

اكتشف الباحثون الأمنيون في فريق عمل **Project Zero** التابع لشركة غوغل ثغرتين أمنيتين في تصميم جميع المعالجات المصممة في العقدين الماضيين وحتى يومنا هذا، حيث أُطلق عليهما اسم ميلتداون **Meltdown** وسبيكتر **Spectre** عبر المدونة الرسمية للمشروع. وقد توضح أن معالجات معظم أجهزة الحاسوب سواء المكتبية أو المحمولة وصولاً إلى الحواسيب السحابية بالإضافة إلى معالجات الهواتف الذكية وبمختلف أنظمة التشغيل من أندرويد **Android** وأيو أس **IOS** وويندوز **Windows** وماك **macOS** ولينكس **Linux** تحوي إحدى الثغرتين على الأقل.

تعتمد تلك الثغرتان الجديدتان على البنية الفيزيائية المكونة لمعالجات إنتل **Intel** وأي إم دي **AMD** و أي أر إم **ARM** لتسمح للقراصنة بالحصول على معلوماتٍ حساسةٍ كمعلومات الحسابات البنكية وكلمات المرور **passwords** الخاصة بالمستخدمين والشركات

وغيرها. قال دانيال غروس **Daniel Gruss** أحد الباحثين الذين اكتشفوا هذا الخلل في جامعة غراتز Graz للتكنولوجيا: "ربما ميلتداون هو من أسوأ الأخطاء التي وجدت في المعالجات على الإطلاق".

ميلتداون

تعني كلمة ميلتداون **Meltdown** الذوبان، حيث تذيب هذه الثغرة القيود التي يفرضها العتاد المادي، أي بمعنى آخر يكسر الحاجز الأساسي بين تطبيقات المستخدم ونظام التشغيل، وهذا ما يمكّن المهاجم من الوصول إلى الذاكرة الأساسية في الوضع المحمي دون الحاجة للحصول على إذنٍ بذلك، وبالتالي تمكنه من سرقة المعلومات من التطبيقات من مثل كلمات المرور ومفاتيح التشفير ومعلومات بطاقة الائتمان والصور والوثائق.

يتطلب تجاوز هذه المشكلة تغييراً في آلية استخدام نظام التشغيل للذاكرة، ومن المتوقع أن تؤدي هذه التغيرات إلى انخفاض سرعة النظام في معالجة بعض المهام إلى 30%.

الأنظمة المتأثرة بميلتداون

لم يتنهِ اختبار جميع المعالجات حتى الآن لحصر الأنظمة المتأثرة بهذه الثغرات، لكن من المؤكد إن ميلتداون موجودٌ بشكل أساسي في الحواسيب المكتبية والمحمولة والسحابيّة، أي تقنيّاً في جميع الأجهزة المزوّدة بمعالجات إنتل **Intel** المصنعة منذ عام 1995 باستثناء رقاقات السيرفرات من نوع إيتانيوم **Itanium** ومعالجات أتوم **Atom** المصنعة قبل عام 2013.

أُثبت حتى الآن تواجد ثغرة ميلتداون في معالجات إنتل فقط، أما معالجات **AMD** و **ARM** لم يثبت تأثرها بعد.

فيديو يبين ميلتداون أثناء العمل

آلية تجسس ميلتداون على كلمة المرور

سبيكتر

تكسر سبيكتر الحاجز بين التطبيقات المختلفة، ما يسمح للمهاجمين بخداع البرامج الخالية من الأخطاء وتسريب بياناتها السريّة، فتمكن من قراءة ذاكرة التطبيقات عالية الأمان بطريقة مخادعة، فعلى سبيل المثال، في حال زيارة موقع ويب يمكن قراءة الكود البرمجي المكتوب بلغة الجافا سكريبت الخاص بالموقع، وبالتالي قراءة عمليات تسجيل الدخول وكلمات المرور المخزنة، كما يعتبر سبيكتر أحد الثغرات صعبة الاستخدام بالنسبة للقراصنة لكنها بالمقابل صعبة الإصلاح وستؤدي إلى مشاكل أكبر على المدى الطويل.

الأنظمة المتأثرة بـ سبيكتر

تحوي جميع الأنظمة تقريباً هذه الثغرة، بما فيها الحواسيب المكتبيّة والمحمولة والسحابيّة، وحتّى الأجهزة الذكيّة، ولنكون أكثر دقّة، جميع المعالجات الحديثة القادرة على التعامل مع تعليماتٍ متعددة. وقد تم تأكيد وجود سبيكتر في معالجات إنتل و **AMD** و **ARM**.

الفارق بين سبيكتر وميلتداون

يعطل ميلتداون الآلية التي تمنع التطبيقات من الوصول إلى ذاكرة النظام العشوائيّة وبذلك تصل التطبيقات إليها، بينما يخدع سبيكتر البرامج للوصول إلى مواقع عشوائيّةٍ في ذاكرتها. كلا الهجومان يستخدمان القناة الجانبيّة للحصول على المعلومات من مواقع الذاكرة التي تم الوصول إليها.

ربما سيتساءل أحدهم عن مدى فاعلية برامج الحماية من الفيروسات في هذه الحالة، عندها يمكن القول إن مكافحة مضادات الفيروسات لهذه الهجومات والثغرات يعد ممكناً من الناحية النظرية إلا أنه من غير الممكن من الناحية العملية، فمن الصعب اكتشاف هذا النوع من الثغرات على عكس البرمجيات الخبيثة المعتادة، ولكن يمكن الكشف عنها لاحقاً بطريقة مقارنة الثنائيات **comparing binaries** بعدما تصبح معروفة يوماً ما.

ومن الجدير بالذكر أن غوغل أبلغت الشركات المتضررة عن عيب سبيكتر في الأول من حزيران/يونيو من عام 2017، وبالرغم من اتفاق كل من غوغل وإنتل على نشر تقرير عن تفاصيل العيب وخطط الإصلاح الممكن اتباعها في التاسع من يناير/كانون الثاني من عام 2018، إلا أنهما أُجبرتا عن التحدث عنهم قبل الموعد المحدد بعد تراجع أسهم إنتل بمقدار 3.4%.

أصدرت شركة إنتل بياناً تضمن أن الشركة بدأت بتوفير تحديثات برمجية **softwares** وتحديثات للملحقات الخاصة بنظم التشغيل أو ما تسمى بالبرمجيات الثابتة **firmware** للتخفيف من آثار هذه الظاهرة، لكن ذلك سيخفض من سرعة وأداء النظام، وبالتالي سوف تخفض من عمر الحاسب المستخدم.

بدأت الشركات السباق لإطلاق التحديثات والباتشات **Patch** لحماية الأجهزة المختلفة من خطر استغلال تلك الثغرات، فأطلقت مايكروسوفت **Microsoft** التحديثات الأمنية في الثالث من كانون الثاني/يناير من العام الجاري للأجهزة الحاسوبية المكتبية والشخصية التي من الممكن تأثرها بثغرة ميلتداون، كما تصحح الشركة خدماتها السحابية، وقد صرحت غوغل أن الهواتف الذكية الحديثة تعمل في الوقت الحالي بنظام محمي من هذه الثغرات.

وأعلنت شركة **AMD** أنه لا مخاطر تهدد منتجاتها في الوقت الحالي، كما صرحت أمازون أن أنظمة الخدمات **EC2** أصبحت محمية بشكل كامل، لكن يتعين على العملاء تحديث أنظمة التشغيل الخاصة بهم.

أمّا شركة أبل **Apple** فقد أعلنت أنّ جميع أجهزة ماك **MAC** وآيفون **Iphone** وآيباد **IPad** تحوي ثغرتي ميلتداون وسبيكتر، وحثّت المستخدمين على عدم استخدام البرامج غير الموثوقة.

من غير الممكن حالياً تأكيد استغلال القراصنة للثغرتين السابقتين، حيث يصعب الكشف عن هكذا اختراقات، فهما لا تتركان أي أثر في ملفات التسجيل. ويقول دان غويدو **Dan Guido** المدير التنفيذي لشركة الاستشارات الأمنية الإلكترونية تريل أوف بيتس **Trail of Bits**، أنه من المتوقع تطوير المستغلين والقراصنة لمجموعة من التعليمات البرمجية بسرعة كبيرة، بحيث تسمح بشن هجمات تستغل نقاط الضعف السابقة. وستعتبر أدوات جديدة تضاف إلى سلسة الأدوات التي يستخدمها القراصنة حول العالم.

بما أن ميلتداون وسبيكتر عبارة عن عيوب فيزيائية، لذلك يعتبر إصلاحها من المهمات الصعبة، في هذه الأثناء من المهم تثبيت آخر التحديثات الأمنية بمجرد توفرها، لأن الأمر لن يستغرق وقتاً طويلاً لكي يبدأ المخترقون وأصحاب النوايا السيئة في استغلال هذه الثغرات الخطيرة.

- التاريخ: 2018-01-05
- التصنيف: تكنولوجيا

#Spectre# Meltdown #سبيكتر #ميلتداون

المصادر

- Meltdown and Spectre
- kaspersky
- the guardian

المساهمون

- ترجمة
  - سارة رسوق
- مُراجعة
  - علي مرعي
- تحرير
  - ليلاس قزيز
- تصميم
  - يوسف سيف
- نشر
  - أنس عبود