دوشنبه 19 اسفند 1398 - 07:03

تراشه‌های اینتل دارای نقص امنیتی غیرقابل اصلاح هستند!

محققان امنیتی کشف کرده‌اند که تراشه‌های شرکت اینتل در هنگام بوت شدن آسیب‌پذیر هستند، بنابراین نمی‌توان آنها را با به روزرسانی سیستم عامل اصلاح کرد.

محققان امنیتی کشف کرده اند که تراشه های شرکت اینتل در هنگام بوت شدن آسیب پذیر هستند، بنابراین نمی توان آنها را با به روزرسانی سیستم عامل اصلاح کرد.

به گزارش ایسنا و به نقل از انگجت، محققان امنیتی نقص دیگری را در تراشه های جدید اینتل کشف کرده اند که کاملاً غیرقابل اصلاح هستند.

این آسیب پذیری در "موتور امنیتی و مدیریتی همگرا"ی(CSME) اینتل قرار دارد که بخشی از تراشه است و کنترل عملکرد بوت-آپ یا بالا آمدن سیستم، سطح قدرت، سفت افزار(firmware) و مهمترین عملکردهای رمزنگاری را کنترل می کند.

ثابت افزار یا سفت افزار در الکترونیک و رایانه، اغلب به برنامه های تقریباً ثابت و نسبتاً کوچک یا ساختمان های داده ای که درون سخت افزار انواع دستگاه های الکترونیک است، گفته می شود. از دستگاه های دارای سفت افزار می توان از ماشین حساب یا کنترل از راه دور، قطعات رایانه شامل دیسک سخت، صفحه کلید، صفحه نمایش های دیجیتال یا کارت های حافظه، ابزارهای دقیق در علم و رباتیک در صنعت نام برد. همچنین دستگاه های پیچیده تری چون تلفن های همراه و دوربین های دیجیتال دارای سفت افزار هستند.

متخصصان امنیتی دریافتند که یک شکاف کوچک امنیتی در این ماژول وجود دارد که می تواند به مهاجمان اجازه دهد کدهای مخرب را به آن تزریق کنند و در نهایت، رایانه شخصی کاربران را فرماندهی کنند.

این آسیب پذیری یکی دیگر از نقص های مجموعه تراشه های جدید اینتل است که به اعتبار این شرکت مشهور آسیب رسانده است. در سال ۲۰۱۸ نیز اینتل با کشف نقص های بزرگی در تراشه های خود روبرو شد که به مهاجمان اجازه می داد اطلاعات را سرقت کنند.

تراشه "CSME" دارای پردازنده، رم و رام خود است و اولین چیزی است که هنگام بالا آمدن رایانه اجرا می شود. یکی از اولین کارهایی که این تراشه انجام می دهد محافظت از حافظه خود است، اما قبل از اینکه این اتفاق بیفتد، یک لحظه کوتاه وجود دارد که در آن آسیب پذیر است و هکرها می توانند از آن استفاده کرده و با رونویسی و ربودن اجرای کد، از آن بهره ببرند.

از آنجا که بوت کد و رم در CPUهای اینتل کدگذاری شده اند، بدون جایگزینی سیلیکون نمی توان آنها را اصلاح یا تنظیم مجدد کرد. این امر باعث می شود تعمیر این آسیب پذیری برای اینتل یا رایانه سازان غیر ممکن باشد.

عملکردهای امنیتی "CSME" به سیستم عامل و برنامه ها اجازه می دهد تا با استفاده از یک "کلید چیپست"، کلیدهای رمزگذاری فایل را به طور ایمن ذخیره کند. اگر یک مهاجم با اجرای کد مخرب بتواند به آن کلید دسترسی پیدا کند، می تواند به همراه برنامه ها به قسمت های اصلی سیستم عامل دسترسی پیدا کند و آسیب جدی در پی داشته باشد.

"مارک ارمولوف" یکی از محققان می گوید: این کلید، مختص پلتفرم نیست. یک کلید واحد برای کل نسل چیپست های اینتل استفاده می شود و از آنجا که این آسیب پذیری نمی تواند اصلاح شود، ما معتقدیم که استخراج این کلید فقط به زمان نیاز دارد. وقتی این اتفاق بیفتد، هرج و مرج کاملاً حاکم خواهد شد. شناسه سخت افزار جعل می شود، محتوای دیجیتال استخراج می شود و داده های دیسک های رمزگذاری شده رمزگشایی می شوند.

با اینکه این به نظر می رسد این یک آسیب پذیری وحشتناک است، اما لازم به ذکر است که بهره برداری از این آسیب پذیری به دانش فنی، تجهیزات تخصصی و دسترسی فیزیکی نیاز دارد. اما وقتی هکرها وارد یک سیستم شوند، می توانند دسترسی از راه دور را بدست آورند.

این آسیب پذیری در مورد تراشه های اینتل که در پنج سال گذشته ساخته شده اند، صدق می کند. اینتل گفته است که از این آسیب پذیری آگاه است و از ماه مه سال ۲۰۱۹ با به روزرسانی هایی درصدد رفع آنها برآمده است.

این غول تراشه ساز می گوید که این به روزرسانی ها باید حملات محلی را کاهش دهند. با این حال هنوز هم حمله مهاجمان ممکن است. به همین دلیل، اینتل می گوید کاربران باید مالکیت فیزیکی سیستم عامل های خود را حفظ کنند.