بیگانه‌ای پرسه می‌زند

ویژگی بوت امن ویندوز ناخواسته به درِب‌پشتی تبدیل شد

دو کارشناس امنیتی به نام‌های MY123 و Slipstream که موفق به شناسایی رخنه‌ای امنیتی در سیستم‌عامل ویندوز شده بودند، اکنون به مایکروسافت در جهت ترمیم این رخنه امنیتی کمک می‌کنند. هکرها به کمک این حفره امنیتی می‌توانند مکانیزم بوت ایمن (Secure Boot) را که در مدت‌زمان راه‌اندازی سیستم‌عامل ویندوز از کامپیوترهای شخصی محافظت می‌کند، دور بزنند. آن‌گونه که مایکروسافت گزارش داده است، Secure Boot یک پروتکل ایمن بوده که حاصل همکاری مشترک مایکروسافت و اعضای صنعت کامپیوتر است.

این مکانیزم به طور خودکار درون میان‌افزار UEFI قرار می‌گیرد و به کامپیوترهای دسکتاپ، همراه و گوشی‌های هوشمند در فرایند راه‌اندازی کمک می‌کند تا به صورت ایمن اجرا شوند. بوت ایمن به‌منظور مبارزه با بوت‌کیت (bootkit) طراحی شد. بوت‌کیت نوع خاصی از بدافزارها است که فرایندهای راه‌اندازی ویندوز را دستکاری می‌کنند. بوت ایمن در راستای مقابله با این گروه از بدافزارها و محافظت از فایل‌هایی که در مدت‌زمان راه‌اندازی ویندوز به مرحله اجرا درمی‌آیند، استفاده می‌شود. اما کدهایی که مایکروسافت به این مکانیزم ایمن اضافه کرده است، خود زمینه‌ساز بروز یک حفره امنیتی شده است. این دو کارشناس امنیتی کشف کرده‌اند که مایکروسافت بعد از عرضه نسخه Windows 10 v1607 Redstone، نوع جدیدی از سیاست‌گذاری را به بوت ایمن اضافه کرده است. مایکروسافت این خط‌مشی جدید را سیاست‌گذاری مکمل نام‌گذاری کرده است.

مطلب پیشنهادی

آسیب‌پذیری وصله شده دروپال هنوز هم مورد سوء استفاده قرار می‌گیرد
سایت‌های دروپالی در معرض خطر؛ هرچه‌سریع‌تر وصله‌های امنیتی نصب شوند!

این دو کارشناس امنیتی ادعا می‌کنند که یکی از این سیاست‌گذاری‌های مکمل می‌تواند در جهت غیرفعال کردن ویژگی بوت ایمن استفاده شود. غیرفعال شدن این ویژگی به معنای آن است که رمزنگاری امضاشده (cryptographically signed) از سوی مایکروسافت برای فایل‌های استفاده‌شده در مدت‌زمان راه‌اندازی سیستم بررسی نمی‌شوند. این سیاست‌گذاری به مهاجم اجازه می‌دهد ویژگی بوت ایمن را به وضعیت «در حال آزمایش» (testsigning) تغییر حالت دهد؛ به‌طوری‌که هکر می‌تواند کنترل فیزیکی یک دستگاه را به لحاظ بارگذاری باینری‌های امضانشده تحت سیطره خود قرار دهد. با انجام این کار فرایند راه‌اندازی سیستم به‌طور کامل در اختیار هکر قرار می‌گیرد و به این شکل او می‌تواند یک بدافزار را همراه با خود سیستم‌عامل اجرا کرده یا حتی سیستم‌عاملی سفارشی طراحی کند.

تحلیل این دو کارشناس نشان می‌دهد، سیاست‌گذاری بوت ایمن در اصل باگی جامانده از گذشته است. به احتمال زیاد، این سیاست‌گذاری همراه با فرایند توسعه ویندوز10 معرفی شده و به طراحان اجازه می‌دهد درایورهای امضانشده را بارگذاری کنند. اما دامنه تهدیدات به‌وجودآمده در خصوص این سیاست‌گذاری آسیب‌پذیر فراتر از حد تصور است؛ به دلیل اینکه فردی موفق شده است سیاست‌گذاری testing را کشف کرده و آن را روی بستر اینترنت منتشر کند. در حال حاضر هر شخصی می‌تواند یک میان‌افزار UEFI را بارگذاری کند و دستگاه‌هایی را که با استفاده از این ویژگی محافظت می‌شودند، تهدید کند. مایکروسافت به‌سرعت یک تغییر داخلی را به مرحله اجرا درآورد و در ماه جولای (مردادماه) وصله (CVE-2016-3287) MS16-096 را منتشر ساخت. اما وصله عرضه‌شده ناقص بود و مایکروسافت مجبور شد وصله دیگری به نام (CVE-2016-3320) MS16-100 را عرضه کند. اما هنوز به‌درستی مشخص نیست آیا وصله عرضه‌شده می‌تواند مشکل به‌وجودآمده را ترمیم کند یا نه.

Slipstream یکی از کاشفان این حفره در این باره گفته است: «این احتمال وجود دارد که وصله دوم آن‌گونه که باید قادر به ترمیم این مشکل نباشد. من وصله دوم را دانلود و مشاهده کردم تعدادی از مشکلات برطرف شده است؛ اما نمی‌توانم به‌طور دقیق بگویم این وصله چه چیزی را ترمیم کرده است. تنها گذشت زمان نشان می‌دهد آیا این مشکل به‌طور کامل برطرف شده است یا نه.» به اعتقاد بسیاری از کارشناسان امنیتی، حفره شناسایی‌شده همان چیزی است که بسیاری از سازمان‌های دولتی به دنبال آن بوده‌اند. با اینکه حفره مذکور یک درِ پشتی رمزنگاری شده نبوده، از آن به عنوان کلید طلایی یاد شده است؛ به سبب آنکه مسیر جدیدی برای ورود به دستگاه‌هایی را هموار می‌سازد که پیش از این با قفل امنیتی قدرتمندی محافظت می‌شدند. اکنون می‌دانیم که اگر شرکت‌های بزرگ دنیای فناوری به درخواست‌های رسمی واکنش مثبت نشان داده و کلیدی طلایی روی محصولات خود قرار دهند، چه اتفاقات ناخواسته‌ای، آن هم در مقیاس بزرگ، به وجود خواهد آمد.

تاریخ انتشار:

07 مهر 1395

نشانی منبع: https://www.shabakeh-mag.com/security/4767