آسیب پذیری Boothole کشف شد؛ میلیاردها سیستم لینوکسی و ویندوزی در خطر - دیجیاتو

پیمان حسنی | پنجشنبه، ۰۹ مرداد ۱۳۹۹

محققان آسیب پذیری جدیدی به نام BootHole شناسایی کرده‌اند که قبل از بالا آمدن سیستم عامل فعال شده و به هکرها دسترسی لجام گسیخته به سیستم را می‌دهد. با اینکه سیستم‌های لینوکسی مستقیماً در معرض خطر این آسیب پذیری هستند، اما به گفته محققان کامپیوترهای ویندوزی از یک دهه گذشته تاکنون نیز در برابر آن آسیب پذیر بوده و هکرها می‌توانند کامپیوتر را بدون هیچ نشانه‌ای هک کنند.

آسیب پذیری BootHole از فرآیند بوت شدن کامپیوتر و سیستم UEFI Secure Boot که باید از فرآیند بوت محافظت کند، سوءاستفاده می‌کند. گوشی‌ها و PCها نرم افزاری به نام بوت لدر (bootloader) دارند که بالا آمدن سیستم عامل و مدهای ریکاوری را مدیریت می‌کند. سیستم UEFI Secure Boot برای محافظت از فرآیند بوت شدن توسعه داده شد تا مجوز اجرای بوت لدرها و فریم‌ورهای معتبر را داده و از اجرای نمونه‌های مخرب جلوگیری کند.

مشکل زمانی رخ می‌هد که خود بوت لدر حاوی باگی باشد که امکان دسترسی سطح بالا به

سیستم عامل را بدهد. این مشکل در بوت لدر GRUB2 که تقریباً در تمام توزیع‌های لینوکس استفاده می‌شود، به چشم می‌خورد. بوت لدر با مجوزهای بیشتری نسبت به روت سیستم عامل یا ادمین اجرا شده و تصدیق آن تنها از طریق گواهینامه امضا کد دیجیتال (Code Signing) یا کد تاییدیه صورت می‌پذیرد. اگر هکر بوت لدر را با نمونه معتبر اما قابل دستکاری تعویض کند، فرآیند Secure Boot فریب خواهد خورد.

آسیب پذیری BootHole به دلیل توافق صنعت کامپیوتر جهت استفاده از گواهینامه UEFI CA مایکروسافت، علاوه بر سیستم‌های لینوکسی تقریباً تمام کامپیوترهای بازار در چند سال اخیر را نیز هدف قرار می‌دهد.

محققان شرکت امنیتی Eclypsium که آسیب پذیری BootHole را کشف کرده‌اند، خواهان بروزرسانی گسترده کامپیوترها شده‌اند؛ اتفاقی که احتمالاً سالها طول خواهد کشید. تا پیش از انتشار بروزرسانی رسمی کاربران می‌توانند با اقداماتی همچون نصب آپدیت‌های امنیتی غیررسمی و مراقب بیشتر در نصب برنامه‌های ناشناس، مانع از فعالیت این آسیب پذیری شوند.

دیجیاتو