رخنه به System Update
آسیب‌پذیری‌های خطرناک جدید کامپیوترهای لنوو

به نظر می‌رسد، مشکلات امنیتی دست از سر محصولات لنوو بر نمی‌دارند. همین چند وقت پیش بود که یک برنامه مخرب روی کامپیوترهای ساخته شده توسط لنوو شناسایی شد، اما باز هم آسیب‌پذیری‌های دیگری توسط شرکت امنیتی IOActive روی محصولات لنوو شناسایی شده‌اند که هر سه آسیب‌پذیری در ارتباط با سیستم به‌روزرسانی لنوو هستند. سازنده کامپیوترهای شخصی وصله‌های امنیتی لازم برای ترمیم این آسیب‌پذیری‌ها ارائه کرده است.

سه ماه پیش بود که سایت‌های مختلف از وجود یک نرم‌افزار مخرب روی کامپیوترهای لنوو خبر دادند، اما بزرگترین سازنده کامپیوترهای شخصی باز هم در مورد اقدامات امنیتی متهم به سهل‌انگاری شده است. شرکت امنیتی IOActive گزارش داده است که آسیب‌پذیری بزرگی را روی سیستم به‌روزرسانی لنوو شناسایی کرده است که به هکرها اجازه دور زدن آزمایشات مربوط به اعتبارسنجی را داده به‌طوری که به آن‌ها این توانایی را می‌دهد تا یک برنامه قانونی و مجاز لنوو را با یک بدافزار مخرب جایگزین کرده و فرمان‌های خود را از راه دور روی آن اجرا کنند. IOActive آسیب‌پذیری‌های شناسایی شده را در گزارش خود به این صورت آورده است:

آسیب‌پذیری CVE-2015-2219

نسخه‌های 5.6.0.27 و پایین‌تر محصولات لنوو به این آسیب‌پذیری آلوده هستند.

این آسیب‌پذیری به یک کاربر محلی با حداقل اختیارات (least privileged) اجازه می‌دهد تا توانایی اجرای دستورات را در قالب یک کاربر سیستمی داشته باشد. برای انجام این‌کار، سیستم به‌روزرسانی شامل یک سرویس به‌روزرسانی به‌نام SUService.exe است. این سرویس با مجوز یک کاربر سیستمی اجرا شده و با System Update ارتباط برقرار می‌کند. سرویس اقدام به ساخت یک name pipe کرده که با استفاده از آن یک کاربر بدون مجوز توانایی ارسال دستورات را برای سرویس دارد. زمانی‌که System Update بدون مجوز نیاز به اجرای یک برنامه با مجوز سطح بالا می‌کند؛ دستورات را به name pipe نوشته و SUService.exe فرمان‌ها را خوانده و آن‌ها را اجرا کند. لنوو برای آن‌که از اجرای خودسرانه دستورات پیشگیری کند از یک سیستم محدود کننده استفاده می‌کند که در آن برای اجرای فرمان‌ها نیاز به تأیید اعتبار(شامل یک نشانه امنیتی) استفاده می‌کند. اما متأسفانه این نشانه امنیتی به راحتی قابل پیش‌بینی بوده و توسط هر کاربری بدون آن‌که مجوزهای لازم را داشته باشد می‌تواند ایجاد شود. در نتیجه یک هکر به آسانی همین فرآیند را در قالب SYSTEM Update می‌تواند انجام دهد. هکر یک نشانه امنیتی معتبر ایجاد کرده و در آن دستورات اجرایی را قرار دهد. در ادامه SUService.exe فرمان را اجرا کرده و به عنوان کاربر SYSTEM در نظر گرفته شود.

اصلاح باگ

لنوو به‌روزرسانی لازم را برای این مشکل عرضه کرده است که در آن روش تصدیق هویت توکن (Token) قبلی را

جایگزین کرده است. این به‌روزرسانی از طریق System Update در دسترس کاربران قرار دارد.

آسیب‌پذیری CVE-2015-2233

نسخه‌های 5.6.0.27 و پایین‌تر محصولات لنوو به این آسیب‌پذیری آلوده هستند.

هکرها با استفاده از این آسیب‌پذیری توانایی دور زدن بررسی‌های مربوط به اعتبارسنجی و امضاء را به صورت محلی و از راه دور داشته و می‌توانند برنامه‌های مورد تأیید لنوو را با برنامه‌های مخرب جایگزین کنند. این برنامه‌ها در ادامه می‌توانند همانند برنامه‌های قانونی به اجرا در آمده و کار کنند. System Update فایل‌های اجرایی را از اینترنت دانلود کرده و آن‌ها را اجرا می‌کند. با استفاده از این آسیب‌پذیری هکرها از راه دور توانایی اجرای یک حمله man-in-the-middle را که امکان جایگزین کردن فایل‌های مخرب را با برنامه‌های لنوو به آن‌ها می‌دهد دارند. اگر صاحب یک دستگاه لنوو اقدام به‌بروزرسانی ماشین مورد استفاده خود در یک مکان عمومی کند، فرد دیگری می‌تواند با استفاده از این حفره امنیتی اقدام به جایگزین کردن برنامه لنوو با برنامه خودش کند، چیزی که محققان امنیتی آن را "حمله کلاسیک کافی‌شاپ" می‌نامند. System Update از TLS/SSL برای ایمن‌سازی ارتباطات با سرور به‌روزکننده و محافظت در برابر حملات سبک کافی‌شاپ استفاده می‌کند. اما مشکل این روش در چیست؟ زمانی‌که فرآیند اعتبارسنجی امضاء انجام می‌شود، لنوو در چرخه اعتبارسنجی CA (مرجع صدور گواهی دیجیتال) دچار مشکل می‌شود. در نتیجه یک هکر می‌تواند یک CA جعلی را ایجاد کرده و از آن برای ساخت یک گواهی code signing استفاده کند. این کد یک فرآیند امضاء دیجیتالی اجرایی و اسکریپتی برای تأیید نویسنده نرم‌افزار و تضمین‌کننده این است که کدهای نرم‌افزار مورد دستکاری قرار نگرفته یا خراب نشده است. System Update در این مکان است که در اعتبارسنجی CA دچار مشکل می‌شود. System Update فایل‌های اجرایی داری امضاء حتی آن‌هایی که گواهی جعلی دارند را قبول کرده و به آن‌ها همچون نرم‌افزارهای عادی اجازه اجرا می‌دهد.

اصلاح شده

لنوو به‌روزرسانی لازم برای این‌که این چرخه اعتبارسنجی به درستی انجام شود؛ عرضه کرده است. این به‌روزرسانی از طریق System Update قابل دریافت است.

آسیب‌پذیری CVE-2015-2233

نسخه‌های 5.6.0.27 و پایین‌تر محصولات لنوو به این آسیب‌پذیری آلوده هستند.

این آسیب‌پذیری به کاربران محلی بدون مجوز این توانایی را می‌دهد تا دستورات مورد نظر خود را همانند یک مدیر اجرا کنند. System Update اجازه دانلود فایل‌های اجرایی از اینترنت و اجرای آن‌ها را می‌دهد. System Update امضاء مربوط به فایل‌ها را قبل از آن‌که اجرا شوند، مورد بررسی قرار می‌دهد. این تکنیک در ظاهر خوب بوده و به درستی عمل می‌کند، اما این‌کار با استفاده از یک دیکشنری که توسط هر کاربری قابل بازنویسی است، انجام می‌شود. یک هکر محلی می‌تواند از این آسیب‌پذیری نهایت استفاده را ببرد، به طوری‌که صبر می‌کند تا System Update اقدام به بررسی صحت امضاء فایل اجرایی کند و سپس فایل اجرایی را با نسخه مخرب قبل از آن‌که System Update توانایی اجرای فایل اجرایی را داشته باشد، جایگزین کند. زمانی‌که System Update آماده اجرای فایل اجرایی می‌شود، در حقیقت نسخه بدافزاری را اجرا می‌کند، با این تفکر که آن یک فایل اجرایی بوده که اصالت آن قبلا مورد تأیید قرار گرفته است. یک هکر از این روش برای به دست آوردن مجوزهای مختلف نیز می‌تواند استفاده کند.

اصلاح شده

لنوو یک به‌روزرسانی برای حل این باگ ارائه کرده است که نحوه دانلود و ذخیره شده فایل‌ها را تغییر می‌دهد. این به‌روزرسانی از طریق System Update قابل دریافت است.

این آسیب‌پذیری‌ها، اولین بار در ماه فوریه توسط متخصصان امنیتی شناسایی شدند، این آسیب‌پذیری‌های مهم باعث شدند تا لنوو از شرکت امنیتی IOActive برای اصلاح آسیب‌پذیری‌ها درخواست کمک کنند. تیم‌های توسعه و امنیت لنوو به طور مستقیم با IOActive برای کار روی آسیب‌پذیری‌های پیدا شده روی محصولات لنوو همکاری کردند.

ماحصل این همکاری دوجانبه عرضه وصله لازم برای حذف این باگ‌ها بود. اما دارندگان دستگاه‌های لنوو برای پیشگیری از خطری که IOActive آن را یک خطر عظیم امنیتی اعلام کرده است باید خود شخصا اقدام به دانلود به‌روزرسانی‌های امنیتی کنند. هر چند لنوو به مشکلات سریعا واکنش نشان می‌دهد، اما پیدا شدن چنین حفره‌های امنیتی برای بزرگ‌ترین سازنده کامپیوترهای شخصی که هر روز سعی در بزرگ‌تر شدن می‌کند، شرم‌آور است.

تاریخ انتشار:

20 اردیبهشت 1394

نشانی منبع: https://www.shabakeh-mag.com/security/629