وصله چندین آسیب‌پذیری بحرانی در HP Support Assistant

خلاصه‌ی خبر:

اخیراً طبق اعلام HP، چندین آسیب‌پذیری مهم در HP Assistant، سیستم‌عامل‌های ویندوز را در معرض حملات اجرای کد از راه دور قرار می‌دهد و می‌تواند به مهاجمان اجازه دهد مجوزهای دسترسی خود را بالا ببرند یا پس از بهره‌برداری موفق، فایل‌های دلخواه را حذف کنند. Bill Demirkapi، محقق امنیتی، ده آسیب‌پذیری مختلف را در نرم‌افزار HP Support Assistant یافت، از جمله پنج نقص در افزایش سطح‌دسترسی محلی، دو آسیب‌پذیری در حذف فایل‌های دلخواه و سه آسیب‌پذیری در اجرای کد از راه دور اما با این حال HP هنوز نتوانسته است سه مورد از آسیب‌پذیری‌های افزایش سطح‌دسترسی محلی را وصله کند و این یعنی که حتی اگر از آخرین نسخه‌ی HP Support Assistant استفاده می‌کنید، همچنان در معرض حملات هستید.

اخیراً طبق اعلام HP، چندین آسیب‌پذیری مهم در HP Assistant، سیستم‌عامل‌های ویندوز را در معرض حملات اجرای کد از راه دور قرار می‌دهد و می‌تواند به مهاجمان اجازه دهد مجوزهای دسترسی خود را بالا ببرند یا پس از بهره‌برداری موفق، فایل‌های دلخواه را حذف کنند.

HP Support Assistant که توسط HP به عنوان "ابزار رایگان کمک‌به کاربر" به بازار عرضه شده است، بر روی دسک‌تاپ‌ها و نوت‌بوک‌های جدید HP بصورت پیش‌فرض نصب شده است و به منظور ارائه‌ی پشتیبانی، به‌روزرسانی و اصلاحات خودکار برای رایانه‌های شخصی و چاپگرها طراحی شده است.

HP می‌گوید: "عملکرد و امنیت رایانه‌های شخصی و چاپگرهای خود را با به‌روزرسانی خودکار سیستم‌عامل و درایور، می‌خواهد بهبود ببخشد." "کاربران می‌توانند گزینه‌های خود را پیکربندی کنند تا به روزرسانی‌ها به صورت خودکار دریافت شده و نصب شوند یا در صورت موجود بودن به شما اطلاع داده‌شود."

رایانه‌های HP فروخته شده پس از اکتبر ۲۰۱۲ و سیستم‌عامل‌های ویندوز ۷، ویندوز ۸ و ویندوز ۱۰، همه HP Support Assistant را به‌طور پیش‌فرض دارند.

برخی از نقص‌های بحرانی وصله شدند ولی برخی دیگر هنوز نه!

Bill Demirkapi، محقق امنیتی، ده آسیب‌پذیری مختلف را در نرم‌افزار HP Support Assistant یافت، از جمله پنج نقص در افزایش سطح‌دسترسی محلی، دو آسیب‌پذیری در حذف فایل‌های دلخواه و سه آسیب‌پذیری در اجرای کد از راه دور.

HP PSIRT پس از دریافت گزارش افشای اولیه از Demirkapi در اکتبر، بخشی از آسیب‌پذیری‌ها را در دسامبر سال ۲۰۱۹ برطرف کرد.

وصله‌ی دیگری نیز در مارس ۲۰۲۰، پس از آنکه محقق گزارش جدیدی را در ژانویه ارسال کرد تا یکی از نقص‌هایی که قبلاً دست نخورده باقی مانده بود را وصله و یک نقص جدید را اصلاح کند، صادر شد.

با این حال HP هنوز نتوانسته است سه مورد از آسیب‌پذیری‌های افزایش سطح‌دسترسی محلی را وصله کند و این یعنی که حتی اگر از آخرین نسخه‌ی HP Support Assistant استفاده می‌کنید، همچنان در معرض حملات هستید.

این نوع آسیب‌پذیری معمولاً در مراحل بعدی حملات توسط مهاجمان مورد استفاده قرار می‌گیرد تا سطح دسترسی را بالا ببرند و ماندگاری خورد را تثبیت کنند. این امر به آنها اجازه می‌دهد تا دستگاه‌های هدف را پس از نفوذ، قربانی کنند و کنترل آن‌ها را بدست‌گیرند.

Demirkapi در شرح مفصل فنی خود توضیح داد: "توجه به این نکته ضروری است که HP نتوانسته است سه آسیب‌پذیری محلی برای افزایش سطح‌دسترسی وصله کند، حتی اگر آخرین نسخه‌ی نرم‌افزار را داشته باشید، هنوز آسیب‌پذیر هستید مگر اینکه عامل را به طور کامل از دستگاه خود حذف کنید."

1. Local Privilege Escalation #1 – Patched ✅
2. Local Privilege Escalation #2 – Unpatched ❌
3. Local Privilege Escalation #3 – "Patched" 😕 (not really)
4. Local Privilege Escalation #4 – Unpatched ❌
5. Local Privilege Escalation #5 – Unpatched ❌
6. Arbitrary File Deletion #1 – Patched ✅
7. Arbitrary File Deletion #2 – Patched ✅
8. Remote Code Execution Variant #1 – Patched ✅
9. Remote Code Execution Variant #2 – Patched ✅
10. Remote Code Execution Variant #3 – Patched ✅

آسیب‌پذیری‌های وصله‌شده و وصله‌نشده (Bill Demirkapi)

اقدامات در جهت کاهش تاثیر منفی نقص‌های وصله‌نشده موجود

Demirkapi توصهی می‌کند که برای کاهش تاثیر منفی نقص‌های وصله‌نشده موجود، باید نرم‌افزارهای آسیب‌پذیر را که شامل *HP Support Assistant* و *HP Support Solutions Framework*/ست از رایانه‌ی خود، لغونصب کنید.

اگر برای به‌روز نگه‌داشتن نرم‌افزار دستگاه‌های خود به آن‌ها متکی هستید، باید بدانید که HP Support Assistant شما را ملزم می‌کند که به‌طور پیش‌فرض به‌روزرسانی‌های خودکار را انتخاب کنید.

اگر به‌روزرسانی‌های خودکار را فعال نکرده‌اید یا نمی‌خواهید آن‌ها را روشن کنید، باید با چک‌کردن آخرین نسخه، برنامه را به صورت دستی به‌روزرسانی کنید یا آخرین نسخه‌ی منتشر شده را با دانلود از HP's support website نصب کنید.

منبع:

https://www.bleepingcomputer.com/news/security/windows-pcs-exposed-to-attacks-by-critical-hp-support-assistant-bugs/