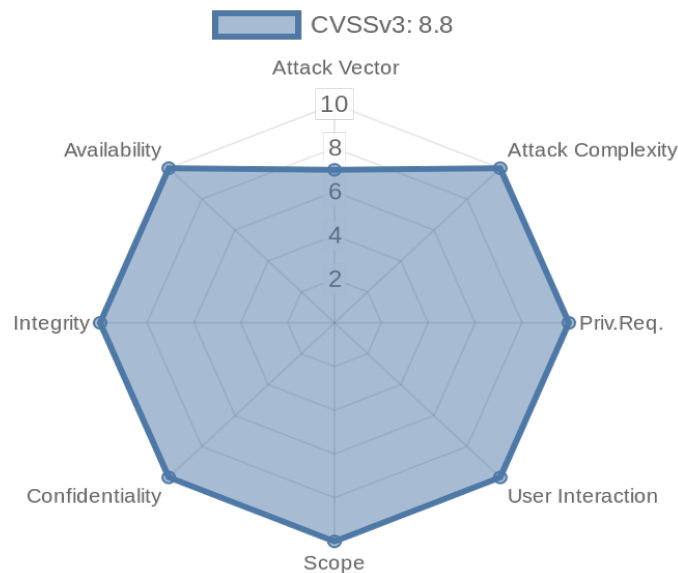


آسیب پذیری ۳۰۰۷۸ - ۲۰۲۴ - CVE

۲ مرداد ۱۴۰۳

۱ مقدمه

آسیب‌پذیری CVE-2024-30078 یک نقص امنیتی جدی در درایور Wi-Fi ویندوز است که امکان اجرای کد از راه دور را برای مهاجمان فراهم می‌کند. این آسیب‌پذیری به مهاجمان اجازه می‌دهد تا بدون نیاز به هیچ گونه تعامل کاربر، کد مخرب را اجرا کنند و به سیستم‌ها دسترسی غیرمجاز پیدا کنند. این مشکل می‌تواند منجر به دسترسی به داده‌ها، نصب نرم‌افزارهای مخرب و سایر اقدامات بدخواهانه شود. این آسیب‌پذیری دارای امتیاز CVSS ۸.۸ از ۱۰ است که نشان‌دهنده شدت بالای آن است. مهاجمان می‌توانند با استفاده از این نقص، کنترل کامل سیستم‌های آسیب‌پذیر را به دست بگیرند. آسیب‌پذیری مذکور تمام نسخه‌های پشتیبانی‌شده ویندوز از جمله ویندوز ۱۰، ویندوز ۱۱ و ویندوز سرور را تحت تأثیر قرار می‌دهد.



CVE-2024-30078

۲ مشخصات حمله

در این بخش، جزئیات مختلف مربوط به آسیب‌پذیری CVE-2024-30078 که در درایور Wi-Fi ویندوز وجود دارد، به تفصیل توضیح داده می‌شود. این اطلاعات شامل بردار حمله، پیچیدگی حمله، نیاز به مجوزها، تعامل کاربر، گستره تأثیر، و تأثیرات بر محرمانگی، یکپارچگی و دسترس‌پذیری است.

بردار حمله : بردار حمله این آسیب‌پذیری، شبکه است. مهاجم می‌تواند با ایجاد یک نقطه دسترسی Wi-Fi مخرب، کد مخرب را به دستگاه قربانی ارسال کند. وقتی دستگاه قربانی به این شبکه متصل می‌شود، کد مخرب اجرا می‌شود.

پیچیدگی حمله : پیچیدگی حمله پایین است. به این معنا که مهاجم نیازی به شرایط خاص یا پیچیده برای بهره‌برداری از این آسیب‌پذیری ندارد. فقط کافیه یک نقطه دسترسی مخرب ایجاد کند و منتظر بماند تا دستگاه قربانی به آن متصل شود.

نیاز به مجوزها : برای بهره‌برداری از این آسیب‌پذیری، نیازی به مجوزهای ویژه یا سطح بالای دسترسی وجود ندارد. مهاجم می‌تواند بدون نیاز به احراز هویت یا دسترسی به سیستم قربانی، کد مخرب را اجرا کند.

تعامل کاربر : هیچگونه تعامل کاربر برای بهره‌برداری از این آسیب‌پذیری نیاز نیست. به محض اینکه دستگاه قربانی شبکه Wi-Fi مخرب را شناسایی کند، کد مخرب به صورت خودکار اجرا می‌شود.

گستره تأثیر : گستره تأثیر این آسیب‌پذیری محدود به دستگاه‌های متصل به شبکه Wi-Fi است. اما با توجه به استفاده گسترده از Wi-Fi در دستگاه‌های مختلف، تأثیر آن می‌تواند بسیار گسترده باشد و بسیاری از دستگاه‌ها را تحت تأثیر قرار دهد.

محرم‌انگی : این آسیب‌پذیری می‌تواند به شدت محرم‌انگی اطلاعات کاربران را به خطر بیندازد. مهاجم می‌تواند به داده‌های حساس دسترسی پیدا کند و آنها را به سرقت ببرد یا افشا کند.

یکپارچگی : یکپارچگی داده‌ها نیز می‌تواند تحت تأثیر قرار گیرد. مهاجم می‌تواند داده‌ها را تغییر دهد یا دستکاری کند که می‌تواند به نتایج نادرست و مخرب منجر شود.

دسترس‌پذیری : این آسیب‌پذیری می‌تواند دسترس‌پذیری سیستم را نیز تحت تأثیر قرار دهد. مهاجم می‌تواند با اجرای کد مخرب، سیستم را قفل کند یا از دسترس خارج کند.

مراجع

Microsoft Security Response Center: CVE-2024-30078 [۱]

National Vulnerability Database: CVE-2024-30078 [۲]

CVE-2024-30078: Unveiling a Dangerous Windows Wi-Fi Driver Remote [۳]

Code Execution Vulnerability

Rapid7: CVE-2024-30078: Windows Wi-Fi Driver Remote Code Execution [۴]

Vulnerability