باسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی چند آسیب‌پذیری مهم در درایورهای گرافیکی اینتل

فروردین۹۹

۱ چکیده

اخیرا شرکت اینتل شش آسیب‌پذیری شدید در درایورهای گرافیکی خود که به مهاجمان اجازه می‌داد تا داده‌های حساس را به سرقت ببرند را وصله کرده است. درایور گرافیکی، نرم‌افزاری است که چگونگی عملکرد اجزای گرافیکی با دیگر قسمت‌های کامپیوتر را کنترل می‌کند. برای مثال، شرکت اینتل درایورهای گرافیکی را برای سیستم‌عامل ویندوز توسعه می‌دهد تا کارهایی از قبیل ارتباط با دستگاه‌های گرافیکی خاص اینتل را انجام دهند. در ادامه به بررسی بیشتر آسیب‌پذیری‌های این درایورها خواهیم پرداخت.

۲ محصولات تحت تاثیر

آسیب‌پذیری‌هایی که اخیرا در درایورهای گرافیکی اینتل شناسایی شده‌اند، در نسخه‌های قبل از 15.40.44.5107، 15.45.30.5103، 26.20.100.7158، 26.20.100.6912، 15.36.38.5117، 15.33.49.5100 و 26.20.100.7212 را تحت تاثیر قرار می‌دهند.

۳ تاثیر آسیب پذیری

اخیرا شش آسیب‌پذیری شدید در درایورهای گرافیکی اینتل شناسایی شده‌اند که در صورت بهره‌برداری، امکان ارتقای مجوز، انکار سرویس و افشای اطلاعات را فراهم می‌کنند. شدیدترین این آسیب‌پذیری‌ها نیز مربوط به یک نقص سرریز بافر است. در سیستم امتیازدهی CVSS، امتیاز ۸.۴ از ۱۰ به این آسیب‌پذیری اختصاص یافته است که نشان می‌دهد شدت آسیب‌پذیری زیاد است. بهره‌برداری از این آسیب‌پذیری، به طور بالقوه به یک کاربر احراز هویت شده امکان می‌دهد تا بتواند از طریق دسترسی محلی، یک انکار سرویس پدید آورد.

۴ مشخصه های آسیب پذیری

شدیدترین آسیب‌پذیری از مجموعه شش آسیب‌پذیری شناسایی شده در درایورهای گرافیکی اینتل، مربوط به آسیب‌پذیری سرریز بافر است که با شناسه CVE-2020-0504 شناخته می‌شود. این آسیب‌پذیری، درایورهای گرافیکی نسخه‌های قبل از 15.40.44.5107، 15.45.30.5103 و 26.20.100.7158 را تحت تاثیر قرار می‌دهد و می‌تواند برای یک کاربر معتبر و با دسترسی محلی، امکان ایجاد یک انکار سرویس را فراهم کند.

سرریز بافر نوعی آسیب‌پذیری است که در آن یک بافر (ناحیه‌ای در حافظه فیزیکی که برای ذخیره موقت داده‌ها در حین جابجایی از آن استفاده می‌شود) که می تواند رونویسی شود، در بخش پشته حافظه (ناحیه‌ای از حافظه فرایند که متغیرهای پویا در آن ذخیره می‌شود) است. از این رو، داده‌های اضافی به نوبه خود فضای مجاور حافظه را خراب می‌کند و می‌تواند اطلاعات دیگر را تغییر داده و در را برای حملات مخرب باز کند. یک آسیب‌پذیری سرریز بافر دیگر با شناسه CVE-2020-0501 نیز در درایور گرافیکی (قبل از

نسخه 26.20.100.6912) وجود دارد که می‌تواند توسط یک کاربر معتبر با دسترسی محلی،به منظور ایجاد حمله انکار سرویس مورد بهره‌برداری قرار گیرد.

اینتل همچنین در درایورهای گرافیکی خود به دو نقص شدید کنترل دسترسی نامناسب در درایورهای گرافیکی خود اشاره کرده است که با شناسه‌های CVE-2020-0516 و CVE-2020-0519 شناخته می‌شوند. این آسیب‌پذیری‌ها به مهاجمان احراز هویت شده (با دسترسی محلی) امکان دهد تا امتیازات خود را افزایش دهند و یا حملات انکار سرویس شکل دهند. همچنین اینتل اخیرا یک آسیب‌پذیری پیمایش مسیر[1] با شدت بالا را وصله کرده است که شناسه CVE-2020-0520 به آن اختصاص یافته است. این آسیب‌پذیری مربوط به فایل igdkmd64.sys در درایورهای گرافیکی اینتل است که نسخه‌های قبل از 15.45.30.5103، 15.40.44.5107، 15.36.38.5117 و 15.33.49.5100 را تحت تاثیر قرار می‌دهد. با بهره‌برداری از این آسیب-پذیری می‌توان امکان افزایش امتیازات و یا حمله انکار را به دست آورد. ششمین آسیب‌پذیری نیز مربوط به بهره‌برداری از بررسی نامناسب شرایط در درایورهای گرافیکی است که شناسه CVE-2020-0505 به آن اختصاص یافته است و نسخه‌های قبل از 15.33.49.5100، 15.36.38.5117، 15.40.44.5107، 15.45.30.5103 و 26.20.100.7212 را تحت تاثیر قرار می‌دهد. بهره‌برداری از این آسیب‌پذیری می‌تواند منجر به افشای اطلاعات و یا حمله انکار سرویس شود.

البته این اولین بار نیست که در درایورهای گرافیکی اینتل، آسیب‌پذیری یافت می‌شود. بلکه سال پیش نیز، اینتل ۱۹ آسیب‌پذیری از جمله دو آسیب‌پذیری شدید با شناسه‌های CVE-2018-12216 و CVE-2018-12214 را وصله کرده بود که به یک کاربر با مجوز بالا، امکان می‌دادند تا بتواند با داشتن دسترسی محلی، کدهای دلخواه را به اجرا درآورد.

۵ اقدامات جهت کاهش شدت آسیب پذیری

اینتل برای رفع آسیب‌پذیری‌های گفته شده، وصله‌هایی ارائه کرده است. به کاربران توصیه می‌شود در اولین فرصت نسبت به به‌روزرسانی درایورهای خود اقدام نمایند.

۶ منابع

[1] https://threatpost.com/intel-windows-10-graphics-drivers/142778/

[2] http://www.kalitutorials.net/2016/08/hacking-wpawpa-2-without.html

[3] https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00315.html

[1] Path traversal