مرکز ماهر

انتشار وصله امنیتی برای آسیب‌پذیری‌های متعدد در NVIDIA GPU Display

گزارش آسیب‌پذیری

سازمان NVIDIA در تاریخ ۲۸ فوریه یک به‌روزرسانی امنیتی برای درایور GPU Display ارائه کرده که آسیب‌پذیری‌های مهم و بحرانی را برطرف می‌کند و در سیستم‌های ویندوزی آسیب‌پذیر می‌تواند منجر به حملات اجرای کد مخرب، ارتقای سطح دسترسی، افشای اطلاعات و منع سرویس شود. بهره‌برداری از حفره‌های امنیتی برطرف شده در این به‌روزرسانی فقط توسط کاربران محلی امکان‌پذیر است و مهاجمان از راه دور امکان بهره‌برداری از آسیب‌پذیری را ندارند.

همچنین به‌روزرسانی منتشر شده شامل دو آسیب‌پذیری با حساسیت متوسط درGPU Display و سه آسیب پذیری در نرم‌افزار گرافیکی vGPU است که می‌تواند منجر به حملات منع سرویس شود.

۱ درباره‌ی آسیب‌پذیری‌ها

جزییات دو مشکل امنیتی در درایور GPU Display با درجه حساسیت 8.4 و 6.7 که سیستم‌های ویندوزی را تحت تاثیر قرار می‌دهد در جدول زیر آمده است:

جدول ۱: آسیب‌پذیری‌های مربوط به درایور NVIDIA GPU Display

شناسه CVE	توضیحات	درجه حساسیت
CVE-2020-5957	آسیب‌پذیری در کامپونت control panel که به مهاجم با دسترسی محلی اجازه‌ی آسیب زدن به فایل‌های سیستمی را می‌دهد و می‌تواند منجر به حملات DoS یا ارتقای سطح دسترسی شود	۸.۴
8CVE-2020-5957	آسیب‌پذیری در کامپونت control panel که به مهاجم با دسترسی محلی اجازه‌ی تعبیه یک فایل DLL را می‌دهد و می‌تواند منجر به حمله‌ی DoS، اجرای کد یا افشای اطلاعات شود	۶.۷

سه مشکل امنیتی دیگر با درجه حساسیت 5.5، 6.5 و 7.8 در نرم‌افزار NVIDIA vGPU وجود دارد که با استفاده از این سه، مهاجم می‌تواند بدون نیاز به تعامل با کاربر برای کسب دسترسی، سطح دسترسی خود را نسبت به آنچه در ابتدا توسط سیستم آسیب‌پذیر به آن اعطا شده، ارتقا دهد. همچین به مهاجمان اجازه می‌دهد تا با حملات منع سرویس، سیستم را برای اجرای کد مخرب یا دسترسی به اطلاعات حساس به طور موقت از دسترس خارج کند. جزییات این سه آسیب‌پذیری در جدول زیر آمده است:

جدول ۲: آسیب پذیری های مربوط به NVIDIA vGPU Software

شناسه CVE	توضیحات	درجه حساسیت
CVE-2020-5959	این آسیب‌پذیری در افزونه‌ی vGPU در virtual GPU Manager واقع شده که در آن مقدار یک شاخص ورودی به درستی ارزیابی نشده است و می‌تواند منجر به حملات DoS شود	۷.۸
CVE-2020-5960	این آسیب‌پذیری یک null pointer dereference در ماژول کرنل (nvidia.ko) در virtual GPU Manager است که می‌تواند منجر به حملات DoS شود	۶.۵
CVE-2020-5961	یک پاکسازی نادرست منابع در یک آدرس اشتباه می‌تواند ماشین مجازی میهمان را تحت تاثیر قرار داده و منجر به حملات منع سرویس شود	۵.۵

۲ نسخه‌های آسیب‌پذیر

همه‌ی نسخه‌های آسیب‌پذیر درایور GPU Display به تفکیک محصول و سیستم عامل در جدول زیر آمده است:

شناسه CVE	محصول نرم افزاری	سیستم عامل	نسخه‌های تحت‌تاثیر	نسخه‌های به‌روزرسانی شده
CVE-2020-5957 CVE-2020-5958	GeForce	ویندوز	همه‌ی نسخه‌های R440 قبل از 442.50	442.50
	Quadro و NVS	ویندوز	همه‌ی نسخه‌های R440 قبل از 442.50	442.50
			همه‌ی نسخه‌های R430 قبل از 432.28	432.28
			همه‌ی نسخه‌های R418 قبل از 426.50	426.50
			همه‌ی نسخه‌های R390 قبل از 392.59	392.59
	Tesla	ویندوز	همه‌ی نسخه‌های R440	وصله امنیتی در ۹ مارس ۲۰۲۰ منتشر خواهد شد
			همه‌ی نسخه‌های R418 قبل از 426.50	426.50

همه‌ی نسخه‌های آسیب‌پذیر نرم‌افزار vGPU به تفکیک محصول و سیستم عامل در جدول زیر آمده است:

شناسه CVE	کامپوننت نرم‌افزار vGPU	سیستم عامل	نسخه‌های آسیب‌پذیر		نسخه‌های به‌روزرسانی شده	
			نسخه درایور	نرم‌افزار vGPU	نسخه درایور	نرم‌افزار vGPU
CVE-2020-5661	درایور گرافیکی vGPU برای سیستم عامل مهمان	ویندوز	442.06	10.1	وصله امنیتی در آوریل ۲۰۲۰ منتشر خواهد شد	
			441.66	10.0		
			432.08	9.2	وصله امنیتی در ۹ مارس ۲۰۲۰ منتشر خواهد شد	
			431.79	9.1		
			412.02	9.0		
			426.26	8.2	426.25	8.3
			426.04	8.1		
			425.26	8.0		
CVE-2020-5961	درایور گرافیکی vGPU برای سیستم عامل مهمان	لینوکس	440.56	10.1	وصله امنیتی در آوریل ۲۰۲۰ منتشر خواهد شد	
			440.43	10.0		
			430.63	9.2	وصله امنیتی در ۹ مارس ۲۰۲۰ منتشر خواهد شد	
			430.46	9.1		
			430.30	9.0		
			418.43	8.2	418.130	8.3
			418.92	8.1		
			418.70	8.0		
CVE-2020-5959 CVE-2020-5660	Virtual GPU Manager	Citrix Hypervisor، VMware vSphere، توزیع Red Hat لینوکس KVM و Nutanix AHV	440.53	10.1	وصله امنیتی در آوریل ۲۰۲۰ منتشر خواهد شد	
			440.43	10.0		
			430.67	9.2	وصله امنیتی در ۹ مارس ۲۰۲۰ منتشر خواهد شد	
			430.46	9.1		
			430.27	9.0		
			418.109	8.2	418.130	8.3
			418.92	8.1		
			418.66	8.0		

برای اطلاع از نسخه نصبی حال حاضر NVIDIA خود راهنمای موجود در لینک زیر را دنبال کنید:

https://nvidia.custhelp.com/app/answers/detail/a_id/2039

همچنین دریافت به‌روزرسانی از طریق لینک زیر امکان پذیر است:

https://www.nvidia.com/Download/index.aspx

۳ مراجع

[۱] https://www.bleepingcomputer.com/news/security/nvidia-fixes-high-severity-flaw-in-windows-gpu-display-driver/