هشدار آسیب‌پذیری			
موضوع	آسیب‌پذیری‌های تخریب حافظه سامانه‌عامل مکینتاش		
شماره هشدار	۱۴	**تاریخ صدور هشدار**	۳ مرداد ۱۳۹۸
تشریح تهدید	اخیرا آسیب‌پذیری از نوع خواندن خارج از محدوده (Out-Of-Bounds Read) و سرریز حافظه هیپ (Heap Buffer Overflow) بر روی برخی از مولفه‌های سامانه‌عامل مکینتاش اپل کشف شده است که این آسیب‌پذیری‌ها به ترتیب اجازه خواهند یک مهاجم از راه دور بتواند وکتورهای حمله دلخواه بر روی دستگاه‌های دارای سامانه‌عامل آسیب‌پذیر اجرا کنند و در برخی شرایط با محوریت مستقرسازی بدافزار سطح دسترسی خود را افزایش بدهند. اولین آسیب پذیری کشف شده که از نوع خواندن خارج از محدوده است، اجازه خواهد داد یک مهاجم اطلاعات حساس بر روی سامانه عامل آسیب پذیر را افشا کند. این آسیب پذیری درون متد RsrcAndXorByteFlag کلاس AMDRadeonX4000_AMDAccelSharedUserClient کشف و شناسایی شده است که به دلیل عدم اعتبارسنجی صحیح دادههای ورودی کاربر خواندن خارج از محدوده حافظه رخ خواهد داد. یک مهاجم با استفاده از این آسیب پذیری و بهره بری از دیگر آسیب پذیری ها می تواند سطح دسترسی خود را بر روی سیستم افزایش بدهد. برای بهره برداری از این آسیب پذیری کافی است مهاجم ابتدا توانایی اجرای کد با سطح دسترسی محدود را داشته باشد، تا بتواند این آسیب پذیری را مورد بهره برداری قرار بدهد و سطح دسترسی خود را به سطح دسترسی کامل برساند. این آسیب پذیری دارای شناسه CVE-2019-8691 و سطح هشدارپذیری 4.7 است. دومین آسیب‌پذیری هم مانند آسیب‌پذیری قبلی از نوع خواندن خارج از محدوده مجاز حافظه است که موجب افشای اطلاعات حساس سیستم خواهد شد. این آسیب‌پذیری در متد راه‌انداز کلاس درایورهای AMD با شناسه AMDRadeonX4000_AMDAccelSharedUserClient کشف و شناسایی شده است که به دلیل عدم اعتبارسنجی ورودهای کاربران رخ خواهد داد. این آسیب‌پذیری دارای شناسه CVE-2019-8692 و سطح هشدارپذیری 4.7 است. سومین آسیب پذیری از نوع سرریز حافظه هیپ در سرویس diskmanagementd سامانه‌عامل مکینتاش کشف و شناسایی شده است که به دلیل اعتبارسنجی نادرست طول ورودی‌ها قبل کپی آنها به درون حافظه هیپ رخ خواهد داد. یک مهاجم می‌تواند با بهره‌برداری از این آسیب‌پذیری سطح دسترسی خود را افزایش بدهد و همچنین در زمینه کرنل کد اجرا کند. این آسیب‌پذیری دارای شناسه CVE-2019-8697 و سطح هشدارپذیری ۸٫۸ است.		
راه‌حل کاهش تهدید	اپل برای تمامی آسیب‌پذیری‌های گزارش شده در این لیست هشدار، به‌روزرسانی و وصله امنیتی ارائه کرده است. برای رفع آسیب‌پذیری‌های مذکور کافی است، سامانه‌عامل را به آخرین وصله‌های امنیتی به‌روزرسانی کنید.		
شناسه آسیب‌پذیری	CVE-2017-3881 CVE-2019-8697 CVE-2019-8692	**شدت آسیب‌پذیری**	میانگین سطح هشدار این گزارش ۶ است.
منابع	https://www.zerodayinitiative.com/advisories/ZDI-19-682/ https://www.zerodayinitiative.com/advisories/ZDI-19-686/ https://www.zerodayinitiative.com/advisories/ZDI-19-685/		