هشدار آسیب‌پذیری			
موضوع	شناسایی آسیب‌پذیری منع سرویس و اجرای کد از راه دور بر روی سامانه‌عامل ویندوز		
شماره هشدار	۲۱	**تاریخ صدور هشدار**	۳۰ شهریور ۱۳۹۸
تشریح تهدید	اولین ضعف امنیتی که به تازگی شناسایی شده است، به مهاجمین درون سیستم اجازه خواهد داد که شرایط منع سرویس‌دهی بر روی سامانه‌عامل ویندوز آسیب‌پذیر ایجاد کنند. شایان ذکر است، یک مهاجم برای اینکه بتواند این شرایط را ایجاد کند، ابتدا باید سطح دسترسی اجرای کد بر روی سیستم را به دست آورد تا در نتیجه این آسیب‌پذیری را مورد بهرهبرداری قرار بدهد. دومین آسیب پذیری که شناسایی شده است، به مهاجمین اجازه خواهد داد با بهره برداری از آسیب پذیری توابع Filter و Join درون VBScript کدهای دلخواه بر روی ماشین قربانی اجرا کنند. اولین آسیب‌پذیری که با شناسه ZDI-CAN-9312 ردیابی می‌شود، درون سرویس Storage Service وجود دارد که یک مهاجم می‌تواند با سوء استفاده از این سرویس محتویات یک پوشه را حذف کند. شایان ذکر است، مهاجم می‌تواند با بهره‌برداری صحیح از این آسیب‌پذیری موجب عدم سرویس‌دهی سامانه‌عامل ویندوز شود. دومین آسیب‌پذیری که با شناسه CVE-2019-1208 ردیابی می‌شود، به دلیل عدم عملکرد صحیح توابع Join و Filter درون VBScript رخ می‌دهند. مهاجم با استفاده از کدهای VBScript می‌تواند موجب رخ دادن آسیب‌پذیری استفاده پس آزادسازی (Use-After-Free) شود و در نهایت با بهره‌برداری از این آسیب‌پذیری بر روی ماشین هدف کدهای دلخواه اجرا کند.		
راه‌حل کاهش تهدید	به منظور رفع آسیب‌پذیری عدم سرویس‌دهی ویندوز کافی است، تعامل برنامه‌های کاربردی با فایل‌های حیاتی را محدود کرد تا در نتیجه برنامه‌ای نتواند با حذف فایل‌های حیاتی موجب اختلال در عملکرد سامانه‌عامل ویندوز شود. برای رفع آسیب پذیری دوم کافی است سامانه عامل را به آخرین وصله های امنیتی به روزرسانی کرد.		
شناسه آسیب‌پذیری	ZDI-CAN-9312 CVE-2019-1208	**شدت آسیب‌پذیری**	۶.۱ ۸.۸
منابع	https://www.zerodayinitiative.com/advisories/ZDI-19-848/ https://www.zerodayinitiative.com/advisories/ZDI-19-831/		