هشدار آسیب‌پذیری			
موضوع	آسیب‌پذیری سرریز بافر هیپ[1] سرویس بلوتوث سامانه‌عامل اندروید		
شماره هشدار	۸	**تاریخ صدور هشدار**	۱۹ تیر ۱۳۹۸
تشریح تهدید	آسیب‌پذیری از نوع سرریز بافر هیپ (Heap-based Buffer Overflow) در تابع hci_len بلوتوث «Bluetooth» سامانه‌عامل اندروید «Android» کشف و شناسایی شده است که به مهاجمین اجازه می‌دهد، بر روی سامانه هدف دارای این ضعف امنیتی کدهای دلخواه از راه دور اجرا کنند. شایان ذکر است، مهاجمان نسبتا از راه دور (طول ارتباطی بلوتوث) می‌توانند سامانه‌عامل اندروید دارای این ضعف امنیتی را مورد بهره‌برداری قرار بدهند. اگر چه این آسیب‌پذیری در سرویس بلوتوث اندروید قابل بهره‌برداری است، اما در هر صورت مهاجم به تعامل با کاربر هدف نیازمند است تا او در نتیجه تعامل انتقال یک فایل مخرب به خودش را قبول کند. این آسیب‌پذیری در پردازش طول پاکت‌های پروتکل بلوتوث است. این ضعف امنیتی به دلیل عدم اعتبارسنجی صحیح طول داده‌های ارائه شده توسط کاربران قبل از کپی داده‌ها درون یک حافظه ثابت از هیپ رخ می‌دهد. یک مهاجم با بهره‌برداری از این آسیب‌پذیری و سرریز کردن حافظه هیپ می‌تواند در زمینه پروسه جاری شلکد خودش را اجرا کند.		
راه‌حل کاهش تهدید	گوگل هنوز برای این ضعف امنیتی در سرویس بلوتوث سامانه‌عامل اندروید وصله امنیتی ارائه نکرده است اما با این حال، تا زمانی که وصله امنیتی برای سامانه‌عامل اندروید توسط گوگل ارائه شود، با محدود کردن تعامل مبتنی بر پروتکل بلوتوث می‌توان سطح تهدید این آسیب پذیری را کاهش داد.		
شناسه آسیب‌پذیری	ZDI-19-640	**شدت آسیب‌پذیری**	۸
منابع	https://www.zerodayinitiative.com/advisories/ZDI-19-640/		

[1] Heap Buffer Overflow