| هشدار آسیب‌پذیری | | | |
|---|---|---|---|
| **موضوع** | شناسایی مجموعه‌ای از آسیب‌پذیری‌ها بر روی محصولات Advantech | | |
| **شماره هشدار** | ۱۹ | **تاریخ صدور هشدار** | ۲۰ شهریور ۱۳۹۸ |
| **تشریح تهدید** | مجموعه‌ای از آسیب‌پذیری‌ها بر روی محصولات Advantech کشف و شناسایی شده‌اند که به یک مهاجم اجازه اجرای کد از راه‌دور بر روی تجهیزات آسیب‌پذیر را می‌دهند. شایان ذکر است، مهاجم برای بهره‌برداری از این مجموعه آسیب‌پذیری نیاز به تصدیق هویت ندارند.<br>گروه اول آسیب‌پذیری‌ها با شناسه CVE-2019-13556 و CVE-2019-13552 به ترتیب در پروسه bwrunrpt.exe و bwrunmie.exe و cnvlgxtag.exe محصول WebAccess شناسایی شده‌اند که از طریق پیام‌های کنترل ورودی و خروجی پروسه webvrpcs در دسترس قرار می‌گیرد. این ضعف امنیتی به دلیل عدم اعتبارسنجی صحیح طول داده‌های دریافت شده قبل کپی به درون بافر پشته و همچنین فراخوانی توابع سیستمی رخ می‌دهد. مهاجم با بهره‌برداری از این آسیب‌پذیری در ادامه خواهد توانست کدهای دلخواه بر روی ماشین اجرا کند.<br>گروه دوم آسیب‌پذیری‌ها به ترتیب در پروسه BwDlgpUp.exe و bwgetval.exe محصول WebAccess شناسایی شده است که از طریق پیام‌های کنترل ورودی و خروجی پروسه webvrpcs در دسترس قرار می‌گیرد. این ضعف امنیتی به دلیل عدم اعتبارسنجی صحیح طول داده‌های دریافت شده قبل کپی به درون بافر پشته رخ می‌دهد. مهاجم با بهره برداری از این آسیب پذیری در ادامه خواهد توانست فایل های روی سامانه آسیب پذیر را حذف کند. | | |
| **راه‌حل کاهش تهدید** | به منظور رفع آسیب‌پذیری‌های شناسایی شده بر روی محصول WebAccess شرکت Advantech کافی است، محصول WebAccess آسیب‌پذیر را به آخرین وصله‌های امنیتی ارائه شده توسط این شرکت به روزرسانی کنید. | | |
| **شناسه آسیب‌پذیری** | CVE-2019-13556<br>CVE-2019-13552 | **شدت آسیب‌پذیری** | ۹.۸<br>۵.۳ |
| **منابع** | https://www.zerodayinitiative.com/advisories/ZDI-19-847/<br>https://www.zerodayinitiative.com/advisories/ZDI-19-846/<br>https://www.zerodayinitiative.com/advisories/ZDI-19-845/<br>https://www.zerodayinitiative.com/advisories/ZDI-19-844/ | | |