

| هشدار آسیب پذیری  |  |                  |
|-------------------|--|------------------|
| موضوع             | شناسایی مجموعه‌ای از آسیب‌پذیری‌ها بر روی محصولات Rockwell   |                  |
| شماره هشدار       | ۲۰   | تاریخ صدور هشدار |
| تشریح تهدید       | <p>مجموعه‌ای از آسیب‌پذیری‌های استفاده پس از آزادسازی (Use-After-Free) بر روی محصولات Rockwell 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 تعامل با هدف دارد تا با ارسال کد اکسپلویت در قالب فایل‌های DOE حمله سمت کاربر انجام داده و در نتیجه بتواند آسیب‌پذیری‌های مذکور را مورد بهره‌برداری قرار بدهد.</p> <p>این آسیب‌پذیری‌ها با شناسه CVE-2019-13510، CVE-2019-13519 و CVE-2019-13521 در پردازش فایل‌های DOE محصول Rockwell Automation Arena Simulation شناسایی شده‌اند که به ترتیب به دلیل عدم بررسی وجود آبجکت‌ها قبل شروع عملیات بر روی آن‌ها و همچنین عدم اعتبارسنجی صحیح داده‌های دریافت شده به وجود آمده‌اند. مهاجم با بهره‌برداری از این آسیب‌پذیری در ادامه خواهد توانست کد و همچنین فرامین دلخواه بر روی ماشین آسیب‌پذیر اجرا کند.</p> |                  |
| راه‌حل کاهش تهدید | <p>به منظور رفع آسیب‌پذیری‌های شناسایی شده بر روی محصول Arena Simulation شرکت Rockwell Automation کافی است، محصول Arena Simulation آسیب‌پذیر را به آخرین وصله‌های امنیتی ارائه شده توسط این شرکت به روزرسانی کنید.</p>   |                  |
| شناسه آسیب‌پذیری  | شدت آسیب‌پذیری   | ۷.۸              |
| منابع             | <p>CVE-2019-13510<br/>           CVE-2019-13519<br/>           CVE-2019-13521</p> <p> <a href="https://www.zerodayinitiative.com/advisories/ZDI-19-802/">https://www.zerodayinitiative.com/advisories/ZDI-19-802/</a><br/> <a href="https://www.zerodayinitiative.com/advisories/ZDI-19-801/">https://www.zerodayinitiative.com/advisories/ZDI-19-801/</a><br/> <a href="https://www.zerodayinitiative.com/advisories/ZDI-19-800/">https://www.zerodayinitiative.com/advisories/ZDI-19-800/</a><br/> <a href="https://www.zerodayinitiative.com/advisories/ZDI-19-799/">https://www.zerodayinitiative.com/advisories/ZDI-19-799/</a> </p>  |                  |