> Podatność w oprogramowaniu AdaptiveGRC

24 kwietnia 2026 | CERT Polska(../../../../author/cert-polska/) | #podatność(../../../../tag/podatnosc/), #ostrzeżenie(../../../../tag/ostrzezenie/), #cve(../../../../tag/cve/)

CVE ID	CVE-2026-4313(https://www.cve.org/CVERecord?id=CVE-2026-4313)
Data publikacji	24 kwietnia 2026
Producent podatnego oprogramowania	C&F
Nazwa podatnego oprogramowania	AdaptiveGRC
Podatne wersje	Wydane przed grudniem 2025
Typ podatności (CWE)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') (CWE-79(https://cwe.mitre.org/data/definitions/79.html))
Źródło zgłoszenia	Zgłoszenie do CERT Polska

Opis podatności

CERT Polska otrzymał zgłoszenie o podatności w oprogramowaniu AdaptiveGRC i koordynował proces ujawniania informacji.

Podatność CVE-2026-4313(https://www.cve.org/CVERecord?id=CVE-2026-4313): AdaptiveGRC jest podatny na atak typu Stored Cross-Site Scripting za pośrednictwem pól tekstowych występujących w formularzach. Uwierzytelniony atakujący może zmodyfikować wartość pola tekstowego w żądaniu HTTP POST. Nieprawidłowa walidacja parametrów po stronie serwera skutkuje możliwością wykonania

dowolnego kodu JavaScript w przeglądarce ofiary. Co istotne, luka ta może umożliwić atakującemu przechwycenie tokenu uwierzytelniającego administratora oraz wykonywanie dowolnych działań z uprawnieniami administracyjnymi, co może prowadzić do dalszej kompromitacji systemu.

Problem występuje w wersjach wydanych przed grudniem 2025.

Podziękowania

Za zgłoszenie podatności dziękujemy Antoniemu Kwietniewskiemu (mBank).

Więcej o procesie zgłaszania podatności można przeczytać na stronie https://cert.pl/cvd/(https://cert.pl/cvd/).

Kontakt

ul. Kolska 12 01-045 Warszawa
ePUAP: /NASK-Instytut/SkrytkaESP
e-Doręczenia: AE:PL-60057-61611-BCEGR-11

e-mail: info@cert.pl(mailto:info@cert.pl)
Zgłaszanie incydentów:
incydent.cert.pl(https://incydent.cert.pl/)
cert@cert.pl(mailto:cert@cert.pl)

Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”