Stored XSS in AdaptiveGRC

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-4313
State	PUBLISHED
Assigner	CERT-PL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 12:17:07 UTC
Updated	2026-04-24 14:39:28 UTC
Description	AdaptiveGRC is vulnerable to Stored XSS via text type fields across the forms. Authenticated attacker can replace the valu

Risk And Classification

Primary CVSS: v4.0 2.4 LOW from cvd@cert.pl

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000250000 probability, percentile 0.069350000 (date 2026-04-25)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	cvd@cert.pl	Secondary	2.4	LOW	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/C...
4.0	CNA	CVSS	2.4	LOW	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CF	AdaptiveGRC	affected 5.420.00 5.420.66 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.444.119 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.448.116 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.453.110 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.454.64 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.455.87 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.456.60 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.499.113 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.420.14 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.423.7 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.444.20 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.448.42 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.449.40 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.453.19 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.454.17 custom	Not specified
CNA	CF	AdaptiveGRC	affected 5.420.00 5.456.20 custom	Not specified

References

Reference	Source	Link	Tags
adaptivegrc.com/pl/wszystkie-procesy-grc-w-jednym-narzedziu	cvd@cert.pl	adaptivegrc.com	
cert.pl/posts/2026/04/CVE-2026-4313	cvd@cert.pl	cert.pl	
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Antoni Kwietniewski (mBank) (en)

There are currently no legacy QID mappings associated with this CVE.