



CVE-2026-31845

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-31845
State	PUBLISHED
Assigner	TuranSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-11 19:16:28 UTC
Updated	2026-04-11 19:16:28 UTC
Description	A reflected cross-site scripting (XSS) vulnerability exists in Rukovoditel CRM version 3.6.4 and earlier in the Zadarma telep

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c

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

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

Version	Source	Type	Score	Severity	Vector
4.0	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	9.3	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/H/I:H/A:N
3.1	CNA	CVSS	9.3	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/H/I:H/A:N
2.0	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	6.4		AV:N/AC:L/Au:N/C:P/I:P/A:N
2.0	CNA	CVSS	6.4		AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

None

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:P/I:P/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Rukovoditel	Rukovoditel CRM	affected 3.6.4	Not specified
CNA	Rukovoditel	Rukovoditel CRM	unaffected 3.7	Not specified

References

Reference	Source	Link	Tags
forum.rukovoditel.net/viewtopic.php	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	forum.rukovoditel.net	
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: Shukrullo Raximov (Mothra) (en)

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report