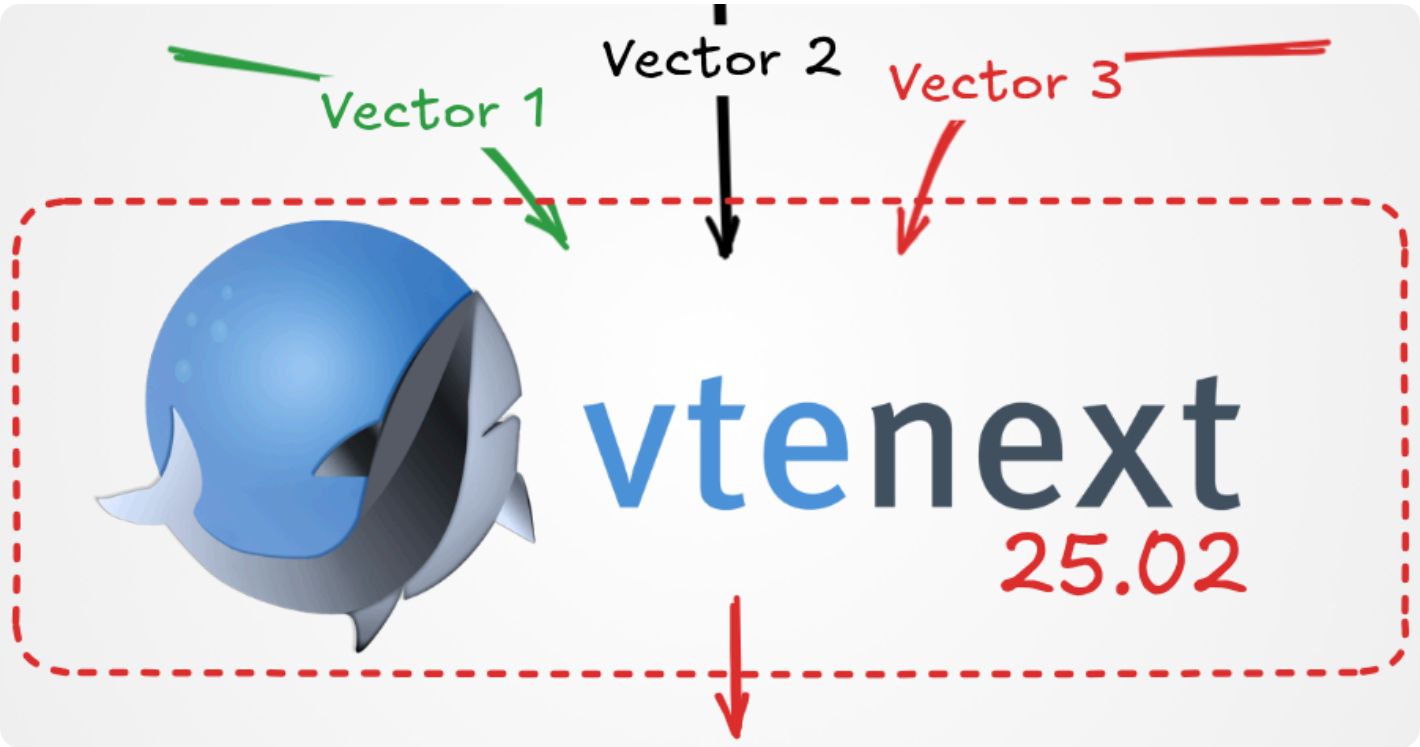
Post

Vtenext 25.02 vulnerability research

Multiple vulnerabilities in vtenext 25.02.1 and prior versions allow unauthenticated attackers to bypass authentication through three separate vectors, ultimately leading to remote code execution on the underlying server.

Posted **Aug 11, 2025** • Updated **Nov 5, 2026**



By **0xbro**

1 min read

Contents >

Summary

Product

VTENEXT CRM

Vendor

vtenext

Severity

Critical

Impact

Authentication Bypass and Remote Code Execution

Affected Version(s)

25.02* and below

Tested Version(s)

20.04, 24.02, 25.02, 25.02.1

First Patched Version

25.02.2

CVE

CVE-2025-71453 - Reflected XSS via `widgetInfoList` in HomeWidgetBlockList

CVE-2025-71454 - CSRF Protection Bypass via HTTP Method Tampering

CVE-2025-71455 - Session Identifier Disclosure via Touch Web Service

CVE-2025-71456 - SQL Injection via `fieldname` in Fax EditView

CVE-2025-71457 - Unverified Password Change via `hub/rpwd.php`

Abstract

> Multiple vulnerabilities in **vtenext 25.02.1** and prior versions allow *unauthenticated* attackers to **bypass authentication** through *three* separate vectors, ultimately leading to **remote code execution** on the underlying server.

You can read the full article on the SicuraNext blog.

Disclosure Timeline

> *Please refer to the disclosure policy page for further details about the disclosure policy adopted by 0xbro.*

- **28/05/2025**: Contacted vtenext for the first time through various communication channels, but did not receive any response.
- **05/06/2025**: Contacted vtenext for the second time, but didn't receive any response again.
- **09/06/2025**: Submitted CVE Request 1879483 to MITRE (never answered).
- **13/07/2025**: Attempted to contact the developers of vtenext via a direct channel on LinkedIn, but without success.
- **24/07/2025**: Vendor released version 25.02.1 containing a silent patch for the Arbitrary Password Reset vulnerability.
- **12/08/2025**: Full disclosure, since a patch exists and the grace period has expired.
- **??/08/2025**: Vendor released version 25.02.2 containing a patch for the other vulnerabilities.
- **04/09/2025**: Following a call with the vtenext team, it was decided to reduce the technical details of the vulnerabilities to give users time to update to the latest version and the team time to patch the remaining vulnerabilities.
- **04/11/2026**: Requested CVE IDs from VulnCheck (CNA), since the MITRE request never received a response.
- **05/11/2026**: VulnCheck published CVE-2025-71453, CVE-2025-71454, CVE-2025-71455, CVE-2025-71456 and CVE-2025-71457.

Disclosed Vulnerabilities

responsible-disclosure php account-takeover path-traversal rce

This post is licensed under **CC BY 4.0** by the author.

Share:

Further Reading

Mar 18, 2026

Exploiting a PHP Object Injection in Profile Builder Pro in the era of AI

WordPress plugin "Profile Builder Pro" (versions before 3.14.5) is susceptible to Unauthenticated PHP Object Injection (CVE-2026-7647). In this blog post, we discuss how we discovered and exploited the vulnerability using …

Nov 13, 2023

Authenticated Static Code Injections in OpenCart (CVE-2023-47444)

In OpenCart versions 4.0.0.0 to 4.0.2.3, authenticated backend users having common/security access and modify privileges can write arbitrary untrusted data inside config.php and admin/config.php, resulting in remote code …

Jul 4, 2020

HackTheBox - Tabby

HackTheBox "Tabby" wirteup is now available!

OLDER

Incorrect Authorization to Authenticated (Contributor+) Multiple Media Actions in Prevent Direct Access Wordpress Plugin (CVE-2025-3861)

NEWER

How I keep updated in the infosec industry

© 2026 **0xbro**. Some rights reserved.
Powered by ☕, 🐛🐜🐞, vulnerabilities and exploits