Kodbox 1.64 Pre-Auth SSRF via Forged ShareOut _check Token

Kodbox 1.64 Pre-Auth SSRF via Forged ShareOut _check Token

Vulnerability Report – VPLUS-2026-12429

1. Basic Information

- **Vulnerability ID:** VPLUS-2026-12429
- **Title:** KodExplorer 4.52: Pre-Auth ShareOut Endpoint Allows Unauthenticated Share Modification via Forged `_check` Token
- **Product:** KodExplorer – Web File Manager
- **Product URL (GitHub):**https://github.com/kalcaddle/kodbox
- **Affected Version:**
  - Confirmed on **Kodbox 1.64**
  - Other versions: not tested
- **Severity:** High
- **Vulnerability Type:** V17 – Missing Authorization / Access Control
- **Authentication:** Pre-Auth (no login required)
- **Confidence:** 99%
- **Verification Status:** Confirmed (reproduced with PoC)
- **CVSS:** Not assigned
- **CVE:** Not assigned
- **Discovery Time:** 2026-02-28 16:38:46

2. Description

In **Kodbox 1.64**, the `explorer/shareOut/shareMake` endpoint uses a `_check` parameter to guard sensitive share-out operations. This parameter is validated via `Mcrypt::decode(..., "kodShareOut")` using a **hard-coded symmetric key**.

Because the key `"kodShareOut"` is embedded in the codebase, any party with access to a KodExplorer installation or source code can **forge valid `_check` tokens offline**. The application then accepts these forged tokens as if they were legitimate, allowing unauthenticated users to call sensitive endpoints that manage external collaboration shares.