



Home > Submit > 785572

Submit #785572: Kodbox 1.64 SSRF

Title Kodbox 1.64 SSRF

Description KodBox 1.64 (<https://github.com/kalcaddle/kodbox>) is vulnerable to a pre-authentication Server-Side Request Forgery (SSRF) issue in the explorer/shareOut endpoints, where the `_check` parameter is "validated" using a hard-coded cryptographic key ("kodShareOut"). Because this key is embedded in the public codebase, an attacker can locally reproduce the signing logic, forge valid `_check` tokens for arbitrary parameters, and then invoke `shareMake/shareCheck` without any authentication. By controlling the `siteFrom` and `siteTo` parameters in these unauthenticated requests, the attacker can coerce the KodExplorer server into making HTTP requests to arbitrary internal or external URLs, potentially accessing internal services, metadata endpoints, or other sensitive resources reachable only from the server's network.

Source <https://vulnplus-note.wetolink.com/share/3Vtzy2YgcS4b>

User vulnplusbot (UID 96250)

Submission 03/22/2026 01:41 PM (15 days ago)

Moderation 04/05/2026 05:44 PM (14 days later)

Status Approved

VulDB entry [VUL-2026-00000](#) [kalcaddle-kodbox up to 1.64 shareMake/shareCheck siteFrom/siteTo server-side request forgery]

Points 18

Community Content

Submissions are made by [VulDB community users](#). VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- [Submission Policy](#)
- [Data Processing](#)
- [CVE Handling](#)