

[Arbitrary File Write / Path Trave...](#)

Description

Arbitrary File Write via Upload ...

Proof of Concept:

Prerequisites:

Step 1: Confirm Upload API Sh...

Step 2: Upload a Normal File fo...

Step 3: Exploit Path Traversal v...

Step 4: Verify Filesystem Write ...

Arbitrary File Write / Path Traversal in CRMEB Java Upload Interface

BUG_Author: Chengxin Xu**Affected Version:** CRMEB Java (1.3.4)**Vendor:** [CRMEB Java GitHub Repository](#)**Software:** [CRMEB Java](#)**Vulnerability Files:**

- `crmeb/crmeb-admin/src/main/java/com/zbkj/a`
- `crmeb/crmeb-`
`service/src/main/java/com/zbkj/service/serv`
- `crmeb/crmeb-common/src/main/java/com/zbkj/`
- `crmeb/crmeb-admin/src/main/java/com/zbkj/a`

Description

CRMEB Java contains an arbitrary file write vulnerability in the upload request. The path from the upload request is used to construct the final filesystem or post-normalization root directory enforcement.

As a result, an attacker can supply traversal sequences such as `../../../../` to be written outside the intended upload subdirectory. In the test case, the path from the expected `/data/uploads/crmebimage/public`

Arbitrary File Write via Upload Endpoints (`/api/admin/upload/file`)

The vulnerability chain starts from the upload endpoints exposed. The `model` parameter is passed directly into `UploadService`

Entry Point (UploadController.java:53-56 and 69-72):