Arbitrary File Write / Path Tra 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 th from the upload request is used to construct the final filesyste or post-normalization root directory enforcement.

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

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

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

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