Description

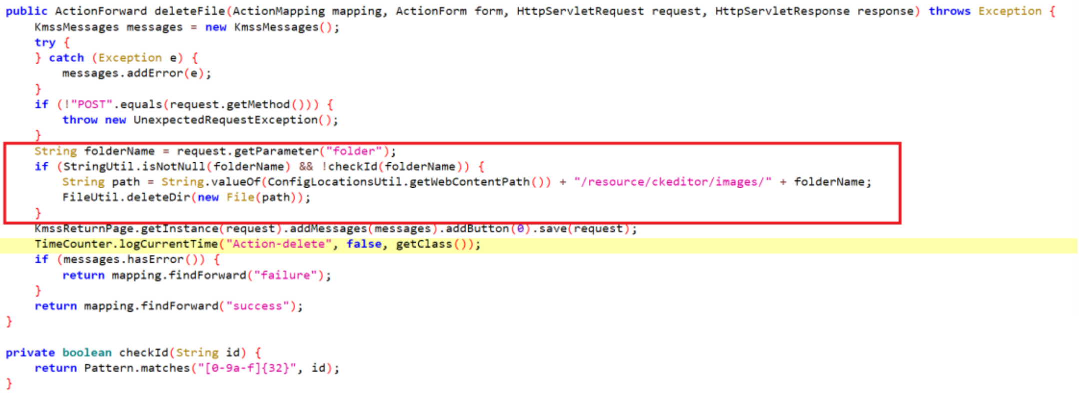
In the Lanling EKP OA application, under ordinary user permissions, the API interface sys/common/import.do?method=deleteFile has directory traversal, which allows arbitrary directory deletion.

Impact

EKP v16, v15

Analysis

The logic of the sys/common/import.do?method=deleteFile interface allows you to delete directories.



```
public ActionForward deleteFile(ActionMapping mapping, ActionForm form, HttpServletRequest request, HttpServletResponse response) throws Exception {
    KmssMessages messages = new KmssMessages();
    try {
    } catch (Exception e) {
        messages.addError(e);
    }
    if (!"POST".equals(request.getMethod())) {
        throw new UnexpectedRequestException();
    }
    String folderName = request.getParameter("folder");
    if (StringUtil.isNotNull(folderName) && !checkId(folderName)) {
        String path = String.valueOf(ConfigLocationsUtil.getWebContentPath()) + "/resource/ckeditor/images/" + folderName;
        FileUtil.deleteDir(new File(path));
    }
    KmssReturnPage.getInstance(request).addMessages(messages).addButton(0).save(request);
    TimeCounter.logCurrentTime("Action-delete", false, getClass());
    if (messages.hasError()) {
        return mapping.findForward("failure");
    }
    return mapping.findForward("success");
}

private boolean checkId(String id) {
    return Pattern.matches("[0-9a-f]{32}", id);
}
```

The checkId function checks the directory name format, which also has problems. I guess it is logical that the deletion will be executed only if the conditions are met. However, the current logic is the opposite, so the directory will be deleted if it contains anything other than numbers and characters.

Steps to reproduce

1. Ordinary users are required to log in to prevent deletion from affecting functions. You can first create a directory under the {web_root}/resource/ directory, such as creating a test222 directory. Use the post method to send the following interface to successfully delete the target directory.

   http://{pre_url}/sys/common/import.do?method=deleteFile&folder=../../test222

Suggestions

1. The request parameters are prohibited from containing directory traversal symbols, '..'
2. After the path is standardized, set a whitelist of directories that can be deleted.