Submit #562902: youkefu https://github.com/zhangyanbo2007/youkefu 1.0 反序列化

Title	youkefu https://github.com/zhangyanbo2007/youkefu 1.0 反序列化
Description	找到 \youkefu-master\src\main\java\com\ukefu\webim\web\handler\admin\system\TemplateController.java 的 impsave 方法，查询结果显示 vulnerable 参数为 “dataFile”。看一下 sink 点并定位它 \youkefu-master\src\main\java\com\ukefu\util\UKTools.java 显示两个 source sink 链的 sink 点都是该方法中调用的 readObject 方法。看一下 sink 点并定位它 \youkefu-master\src\main\java\com\ukefu\util\UKTools.java 显示两个 source sink 链的 sink 点都是该方法中调用的 readObject 方法。核心逻辑在 \ youkefu master \ src \ main \ java \ com \ ukefu \ webm \ web \ handler \ admin \ sy 在 stem \ Template Controller 的第 68-77 行。java 中，接口收到 dataFile 参数后，首先检查 dataFile 参数的值是否为空。如果它不为空，则调用 UKTools.toObject 方法来处理传入的 dataFile 数据，并将处理后的返回值转换为名为 templateList 的 Listcolumn 对象。第 70-76 行是对 templateList 的作。最后，第 77 行重定向到 /admin/template/id ex.exe页面。通过以上分析发现，在从 source 到 sink 的反序列化过程中，没有对 da taFile 参数进行安全处理，因此这里存在反序列化漏洞。
Source	⚠️ https://github.com/Serein123y/vulnerability/blob/main/vul.md
User	Serein123y (UID 84459)
Submission	04/21/2025 09:10 AM (14 days ago)
Moderation	05/04/2025 09:08 AM (13 days later)
Status	Accepted
VulDB Entry	307364 [zhangyanbo2007 youkefu up to 4.2.0 TemplateController.java impsave dataFile deserialization]
Points	20

Notice

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