瑞友天翼应用虚拟化系统远程代码执行漏洞

2023 年 4 月 13 日

一、漏洞概要

漏洞名称	瑞友天翼应用虚拟化系统远程代码执行漏洞
发布时间	**2023 年 4 月 13 日**
组件名称	瑞友天翼应用虚拟化系统
影响范围	**5.x ≤ Ruiyou Tianyi ≤ 7.0.2.1**
漏洞类型	远程代码执行
利用条件	**1、用户认证：不需要用户认证** **2、前置条件：无** **3、触发方式：远程**
综合评价	<综合评定利用难度>：容易。 <综合评定威胁等级>:高危,能造成远程代码执行。
官方解决方案	已发布

二、漏洞分析

2.1 组件介绍

瑞友天翼应用虚拟化系统是由西安瑞友信息技术资讯有限公司研发的具有自主知识产权的应用虚拟化平台，基于服务器计算架构。该系统可以将用户的各种应用软件集中部署在瑞友天翼服务器(群)上，客户端通过 WEB 即可快速安全地访问经服务器上授权的应用软件，实现集中应用、远程接入、协同办公等功能。用户可以享受到集中、便捷、安全、高效的虚拟化功能。

2.2 漏洞描述

2023 年 4 月 11 日，深信服安全团队监测到一则瑞友天翼应用虚拟化系统存在远程代码执行漏洞的信息，漏洞威胁等级：高危。

该漏洞是由于瑞友天翼应用虚拟化系统存在缺陷，攻击者可利用该漏洞在未授权的情况下，构造恶意数据进行远程代码执行攻击，最终获取服务器最高权限。

三、影响范围

目前受影响的瑞友天翼应用虚拟化系统版本：

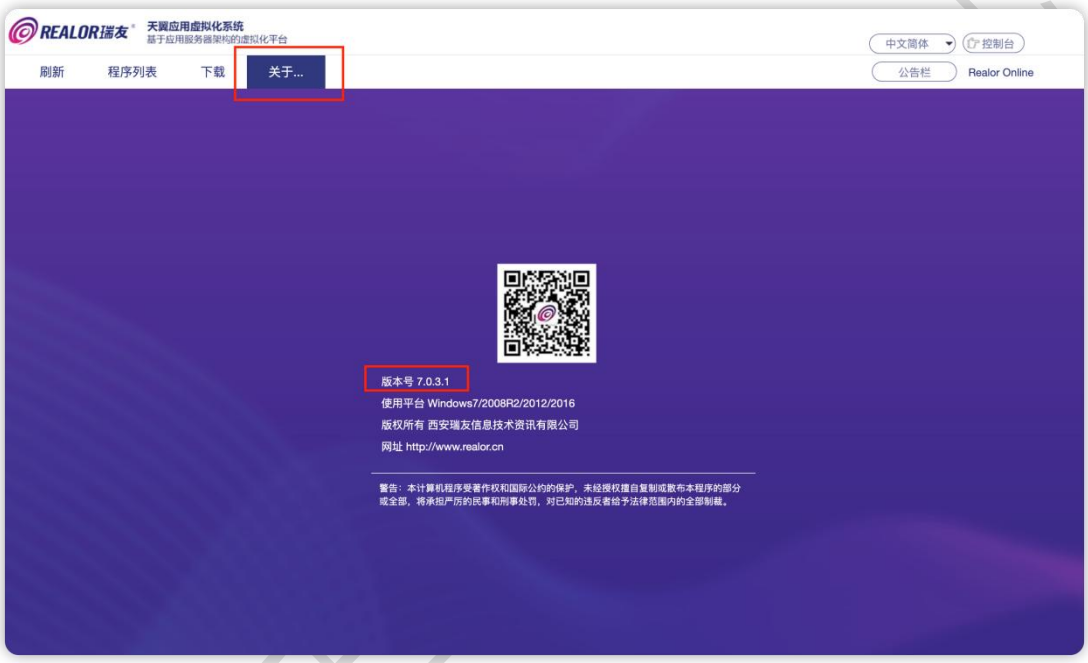
5.x ≤ Ruiyou Tianyi ≤ 7.0.2.1

四、解决方案

4.1 修复建议

1. 如何检测组件系统版本

访问系统 web 页面路径 /CASMain.XGI?cmd=About，点击关于即可查看瑞友天翼应用虚拟化系统版本。



2.官方修复建议

当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下：

http://soft.realor.cn:88/Gwt7.0.3.1.exe

4.2 深信服解决方案

1.风险资产发现

支持对 瑞友天翼应用虚拟化系统的主动检测，可批量检出业务

场景中该事件的**受影响资产**情况，相关产品如下：

【深信服云镜 YJ】已发布资产检测方案。

2.漏洞主动检测

支持对瑞友天翼应用虚拟化系统远程代码执行漏洞的主动检测，可**批量快速检出**业务场景中是否存在**漏洞风险**，相关产品如下：

【深信服云镜 YJ】预计 2023 年 4 月 17 日发布检测方案。

【深信服漏洞评估工具 TSS】预计 2023 年 4 月 17 日发布检测方案。

【深信服安全托管服务 MSS】预计 2023 年 4 月 17 日发布检测方案。

【深信服安全检测与响应平台 XDR】预计 2023 年 4 月 17 日发布检测方案。

3.漏洞安全监测

支持对瑞友天翼应用虚拟化系统远程代码执行漏洞的监测，可依据流量收集**实时监控**业务场景中的**受影响资产情况，快速检查受影响范围**，相关产品及服务如下：

【深信服安全感知管理平台 SIP】预计 2023 年 4 月 14 日发布检测方案。

【深信服安全托管服务 MSS】预计 2023 年 4 月 14 日发布检测方案。

【深信服安全检测与响应平台 XDR】预计 2023 年 4 月 14 日发布检测方案。

4.漏洞安全防护

支持对瑞友天翼应用虚拟化系统远程代码执行漏洞的防御，**可阻断攻击者针对该事件的入侵行为**，相关产品及服务如下：

【深信服下一代防火墙 AF】预计 2023 年 4 月 14 日发布检测方案。

【深信服 Web 应用防火墙 WAF】预计 2023 年 4 月 14 日发布检测方案。

【深信服安全托管服务 MSS】预计 2023 年 4 月 14 日发布检测方案。

【深信服安全检测与响应平台 XDR】预计 2023 年 4 月 14 日发布检测方案。

五、时间轴

2023/4/11 深信服监测到瑞友天翼应用虚拟化系统远程代码执行漏洞攻击信息。

2023/4/11 深信服千里目安全技术中心发布漏洞通告。

2023/4/13 深信服千里目安全技术中心发布二次漏洞通告。

六、了解更多

深信服千里目安全技术中心持续紧跟国内外漏洞威胁情报，从中筛选出能给客户带来威胁的漏洞，第一时间推送解决方案，持续提供可感知的安全感。在这场永不停歇的攻防战争中，深信服千里目安全技术中心掌握一手漏洞情报，坚持“千里之外，洞悉风险”，与各大网络安全厂商一同维护网络安全，构建平衡、和谐的网络生态系统。关注深信服千里目安全技术中心微信公众号，第一时间了解更多漏洞情报。