奇安信
新 一 代 网 络 安 全 领 军 者

# VRV EDP

# 远程命令执行漏洞

# 安全风险通告二次更新


**奇安信 CERT**

**2021 年 1 月 5 日**

# 目录

# 第1章 安全通告

尊敬的客户：

近日，奇安信 NGSOC 捕捉到 VRV EDP 远程命令执行漏洞，未经身份验证的攻击者通过 VRV 私有协议对开放 22105 端口的主机发送加密处理过的恶意数据，从而实现远程命令执行，控制远程主机。经过奇安信 CERT 研判，此漏洞危害巨大。奇安信 CERT 强烈建议受影响用户及时进行紧急修复，做好相应防护。

当前漏洞状态：

| 细节是否公开 | PoC 状态 | EXP 状态 | 在野利用 |
| --- | --- | --- | --- |
| 否 | 未公开 | 未公开 | 是 |

奇安信 CERT 将持续关注该漏洞进展，并第一时间为您更新该漏洞信息。

# 第2章 文档信息

| | |
|---|---|
| 文档名称 | VRV EDP 远程命令执行漏洞安全风险通告二次更新 |
| 关键字 | 远程命令执行 |
| 发布日期 | 2021 年 1 月 5 日 |
| 分析团队 | 奇安信威胁情报中心、奇安 NGSOC 威胁建模团队、奇安信 CERT |

# 第3章 漏洞信息

## 3.1 漏洞描述

北信源主机监控与补丁分发系统（北信源内网安全管理及补丁分发准入控制系统），以终端管理为核心，形成集主机监控审计、补丁管理、桌面应用管理、信息安全管理、终端行为管控等终端安全行为一体的管理体系，为企业管理者提供终端多位一体、统一管理的解决方案，为用户创建一个安全、可靠、稳定的办公网络。

近日，奇安信 NGSOC 捕捉到 VRV EDP 远程命令执行漏洞，未经身份验证的攻击者通过 VRV 私有协议对开放 22105 端口的主机发送加密处理过的恶意数据，从而实现远程命令执行，控制远程主机。经过奇安信 CERT 研判，此漏洞危害巨大。奇安信 CERT 强烈建议受影响用户及时进行紧急修复，做好相应防护。

奇安信分析团队第一时间复现了 VRV EDP 远程命令漏洞，复现截图如下：

## 3.2 风险等级

**奇安信 CERT 风险评级为：高危**

**风险等级：蓝色（一般事件）**

# 第4章 影响范围

VRV EDP 全版本

# 第5章 处置建议

请联系厂商获取补丁更新：http://www.vrv.com.cn/

或采取奇安信产品解决方案

临时建议：封禁 22105 端口，限制除 VRV 服务端以外的主机与其通信。

# 第6章 产品解决方案

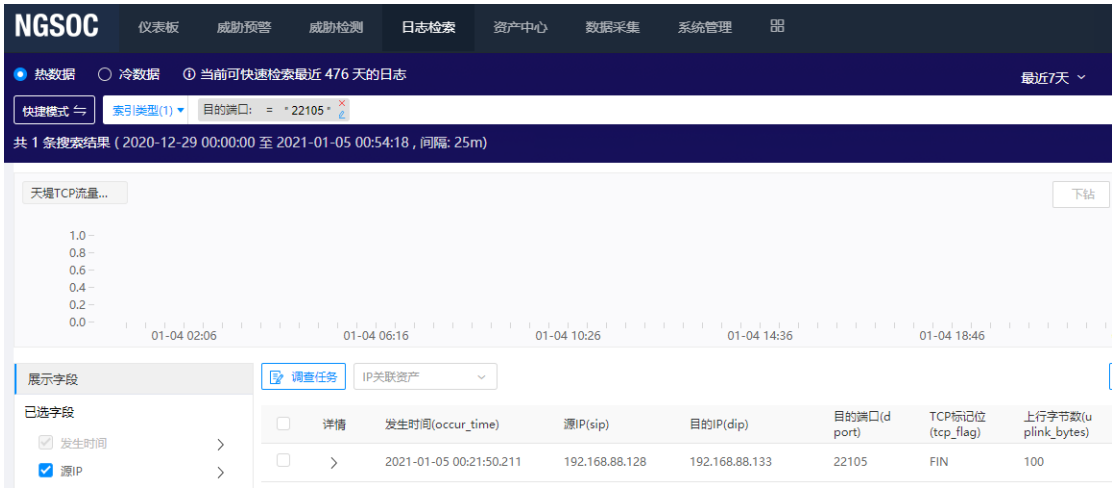
## 6.1 奇安信 NGSOC 解决方案

**奇安信 NGSOC 已支持对该事件相关后门的检测**，请参照以下信息及时升级 NGSOC 网络流量传感器规则库。

| | |
|---|---|
| **探针规则库版本** | ips_2101042359 及以上版本 |
| **规则库获取地址** | https://ngfwup.sg.qianxin.com/offline/download/ |
| **相关规则** | 规则名称: VRV EDP 任意命令执行漏洞<br>规则 ID：51899 |

**流量特征回溯**

在 NGSOC 日志检索查看近 14 天（14 天之前的数据在冷数据查询）天堤 TCP 流量日志热数据，是否有可疑 IP 地址同装有 VRV EDP 客户端的终端进行过网络通信。若存在相关通信行为，请及时反馈！



## 6.2 奇安信网神统一服务器安全管理平台更新入侵防御规则库

奇安信网神虚拟化安全轻代理版本可通过更新入侵防御规则库 2021.01.12 版本，支持对 VRVEDP 远程命令执行漏洞防护，当前规则正在测试中，将于 1 月 12 日发布，届时请用户联系技术支持人员获取规则升级包对轻代理版本进行升级。

奇安信网神统一服务器安全管理平台可通过更新入侵防御规则库 10322 版本，支持对 VRVEDP 远程命令执行漏洞的防护，当前规则正在测试中，将于 1 月 12 日发布，届时请用户联系技术支持人员获取规则升级包对融合版本进行升级。

## 6.3 奇安信网神智慧防火墙产品防护方案

奇安信新一代智慧防火墙（NSG3000/5000/7000/9000 系列）和下一代极速防火墙（NSG3500/5500/7500/9500 系列）产品系列，已通过更新 IPS 特征库完成了对该漏洞的防护。建议用户尽快将 IPS 特征库升级至” 2101051000” 及以上版本并启用规则 ID: 1226601 进行检测。

## 6.4 奇安信网神网络数据传感器系统产品检测方案

奇安信网神网络数据传感器（NDS3000/5000/9000 系列）产品，已具备该漏洞的检测能力。规则 ID 为：51899，建议用户尽快升级检测规则库至 2101042359 以后版本并启用该检测规则。

## 6.5 奇安信天眼产品解决方案

奇安信天眼新一代威胁感知系统在第一时间加入了该漏洞的检测规则，请将规则包升级到 3.0.0105.12567 及以上版本。规则名称：北信源 VRVEDP 远程命令执行漏洞，规则 ID：0x5d91。奇安信天眼流量探针（传感器）升级方法：系统配置->设备升级->规则升级，选择“网络升级”或“本地升级”。

# 第7章 参考资料

[1] http://www.vrv.com.cn/

# 奇安信 CERT

## 【我们是谁】

奇安信应急响应部（又称：奇安信 CERT，奇安信 A-TEAM）成立于 2016 年，是属于奇安信旗下的网络安全应急响应平台，平台旨在第一时间为客户提供漏洞或网络安全事件安全风险通告、响应处置建议、相关技术和奇安信相关产品的解决方案。

奇安信 A-TEAM：团队主要致力于 Web 渗透、APT 攻防、对抗，前瞻性攻防工具预研。从底层原理、协议层面进行严肃、有深度的技术研究，深入还原攻与防的技术本质，曾多次率先披露 Windows 域、Exchange、WebLogic、Exim 等重大安全漏洞，第一时间发布相关漏洞风险通告及可行的处置措施并获得官方致谢。欢迎有意者加入！

## 【我们的服务】

安全风险通告：奇安信 CERT 成立至今已发布上百篇安全风险通告，从成立至今，针对多个高危漏洞、网络安全事件发布风险通告并给出了有效的安全措施。我们的安全研究团队将实时跟踪安全热点事件和漏洞，始终站在用户的视角去评估风险，致力于第一时间向客户发送有效的风险和相关解决方案。

## 【订阅方式】

发送接收邮箱和所属单位至：

cert@qianxin.com

## 【微信公众号】

奇安信 CERT