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　告

：

，　　，

主

，从　　，　　主　。　　，

。　　，　　。

：

	PoC	EXP	

，　一　为　　。

第2章 文　信息

	二
	中　、　　、

第3章　　信息

3.1

主　　与　丁　　（　　丁
），　　为　，　　主　　、　丁　、
、　　、　为　　为一　　，为　业
一　、　一　　，为　　一个　、　、
。

，　　，
主
，从　　，　　主　。　　，
。　　，　　。
一　　了　　，　　下：

3.2

第4章 影响　围

第5章 处　建

丁　：

产

临　：　，　主 与　。

第6章 产品　决

6.1 奇安信 NGSOC　决

NGSOC　事　，　下

。

探针规则库版本

6.2 奇安信 一 务器安全 平台 入侵 御 则库

，，中，于，人。

一

，，中，于，人。

6.3 奇安信 慧 墙产品 护

一（）下一（）产，了。”“上。

6.4 奇安信 据传感器 产品

（）产，。为：，。

6.5 奇安信天　产品　决

一　　一　　了　　，

上　。　：

，　：　。　（　）　：

，　“　”　“　”。

第7章 参　　料

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　　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、E change、WebLogic、E im 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】

：

【微信公众号】

CERT