

每日网安情报速递【20250216】

一、金融业网络安全事件

暂无

二、重大网络安全事件

1. bshare分享插件被黑？百万级网站被劫持事件

- 奇安信发现很多站点在晚上9点至凌晨5点使用安卓UA的设备访问时，会跳转至同一恶意网页。经分析发现这些网页都引用了名为bshare的分享按钮插件，该插件对应的服务域名为static.bshare.cn。最后通过对域名static.bshare.cn的分析，确认这是一起通过抢注过期通用插件服务域名来实施大范围网页劫持的攻击事件。所有直接或间接使用了bshare分析插件的网页都会受到影响。根据评估，恐怕会影响百万级别的网页。奇安信威胁情报中心提醒目前仍在使用bshare插件的用户，需要尽快更换或者停用bshare分享插件。
 - 初步排查我行未使用该组件，不受该事件影响，网安中心将持续关注。
-

三、重大数据泄露事件

1. OmniGPT 聚合类 AI 平台疑遭黑客入侵，3400 万条聊天记录遭泄露

- 用户Gloomer在 BreachForums 上发布帖子，声称自己成功入侵 AI 平台 OmniGPT，获取了一系列用户隐私信息，涉及 3 万名用户电子邮件、电话号码以及 3400 万条用户对话记录。OmniGPT 实际上是一款整合了各大厂商 API 的 AI 聚合平台，包含 ChatGPT-4、Claude 3.5、Perplexity、Gemini 等模型，提供团队协作工具、数据管理和图片分析等。HackRead 调查团队分析黑客公开的平台隐私信息，发现黑客所述内容属实，这些隐私信息涉及用户生活日常、云盘分享链接，账号信息、账单信息和 API 密钥、学生文凭 等。
-

四、重大漏洞风险提示

暂无