atrust nodejs模板渲染注入(SSTI)导致内网漫游

危害级别	严重 AV：远程网络 AC：无-已武器化 PR：需要认证-'无需应用访问配置权' C：完全地 I：完全地 A：完全地
影响产品	aTrust < 2.1.20
涉事单位	深信服科技股份有限公司
所在省份	广东省
所在城市	深圳市
CNVD-ID	暂未报送
CVE ID	暂未报送
参考链接	https://github.com/
影响对象类型	通用型漏洞 - 盒子产品、应用程序、安全产品 www.sangfor.com.cn/product-and-solution/sangfor-security/aTrust 涉及江苏银行集团，广州视源，上海环境等公司
漏洞类型	SSTI
是否已告知厂商	是
报送厂商时间	2022-03-16
漏洞描述	**1. atrust后端存在SSTI(模板渲染注入)导致可以实现内网请求** **2. 可执行写动作接口，可读接口返回数据，访问任意IP,PORT，包括设备内部，如操作数据库接口** **3. 绕过边界访问控制，实现对被保护网络的不可信访问,否认性访问,与产品介绍页描述的'可信访问'的核心能力冲突,且无日志痕迹无法HW溯源** **4. atrust是深信服主打边界安全产品，此问题会破坏产品全局业务和安全效果，对设备与客户安全尤为关键** **5. 需登录，但无需任何高权限，仅最低权限下配置有XX功能可利用，'无边界控制权'(无权配置应用访问)的低权限登陆者，也可突破网络访问限制**
漏洞附件	**http://xxxx.com/video.mp4, 联系微信获取**

1. 在报送漏洞公告信息时，力争保证每条报送的准确性和可靠性。

2. 厂商选择收录后，提供完整的报告或EXP，会与报送时提交的POC所描述的产品版本，演示情况完全匹配。

3. 厂商选择不收录，或恶意收录，按照国家相应法规要求，合法披露报送相关poc, exp。

4. 默认的，一个工作周无反馈为厂商不收录情况。

5. 采纳和实施相应建议则完全由厂商自己决定，其可能引起的问题和结果也完全由厂商承担。是否采纳我们的建议取决于您个人或您企业的决策，您应考虑 其内容是否符合您个人或您企业的安全策略和流程。

厂商验证信息	厂商确认 是否验证通过
厂商是否收录	厂商确认 是否收录
公开日期	厂商确认 是否公开
漏洞解决方案	暂无
厂商补丁	暂无

（编辑：CN赛博） | 已有0条评论

漏洞评分 ： 待定