# 网络与信息安全情况通报

第 9 期

丽江市网络与信息安全监测预警通报中心　　2020 年 5 月 8 日

## 关于 SaltStack 软件存在高危漏洞的预警通报

近日，据国家网络与信息安全信息通报中心监测发现，服务器基础架构集中化管理软件 SaltStack 存在认证绕过漏洞（漏洞编号：CVE-2020-11651）和目录遍历漏洞（漏洞编号：CVE-2020-11652）。经分析研判，攻击者可利用认证绕过漏洞绕过 SaltStack 的验证逻辑，调用相关未授权函数，实现远程命令执行。攻击者可通过构造恶意请求，利用目录遍历漏洞，读取服务器上任意文件。受影响的软件版本包括：版本号低于 2019.2.4 和 3000.2 的 SaltStack 版本。

鉴于该事件影响范围大，危害程度高，请各单位高度重视，立即采取以下防范措施：**一是**及时升级 SaltStack 软件版本，消除安全隐患，升级地址为：https://repo.saltstack.com；

**二是**设置访问控制策略，限制非信任 IP 访问 SaltStack 软件服务 4505 和 4506 端口；三是发现存在数据泄露等安全事件的，及时联系公安网安部门，联系电话：5120626。

送：市直各委、办、局

市级各重要信息系统运营使用单位及行业主管部门。

抄：市公安局警令部，科信处，县（区）网安大队。

承办单位：丽江市网络与信息安全监测预警通报中心　　电话：5120626