关于 SaltStack 软件存在高危漏洞的预警通报

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运维管理软件 SaltStack 存在认证绕过漏洞（CVE-2020-11651）和目录遍历漏洞（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。

鉴于上述漏洞潜在危害较大，建议各重要行业部门和各市（州）公安机关立即采取以下措施：**一是**迅速通报本部门、本行业、本辖区重点单位排查 SaltStack 软件使用情况；**二是**在确

保安全的前提下，及时升级 SaltStack 软件版本，消除安全隐患，升级地址为：https://repo.saltstack.com；三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。相关排查情况请于本周五（5 月 8 日）前反馈公安厅网安总队，发现攻击情况第一时间处置并报告公安厅网安总队。