|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 278 | | |
| 漏洞名称 | SSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】 | 危险级别 | 低 |
| 主机IP | 146.4.80.190、146.4.80.191、146.4.80.196 | | |
| 整改建议 | 目前厂商已经发布了升级补丁以修复这个安全问题，补丁下载链接：OpenSSH-------https://downloads.ssh.com/临时解决方法：\* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 | | |
| 整改情况 | 未整改 | | |