A2020-G是否涉及以下漏洞CVE-2020-15778 CVE-2021-41617 CVE-2023-38408 CVE-2023-51767 CVE-2018-15919 CVE-2017-15906 CVE-2020-14145 CVE-2018-20685 CVE-2018-15473 CVE-2023-48795 CVE-2019-6111 CVE-2019-6109

堡垒机 ZL_qiufeng 2024-08-25 发表

问题描述

如标题

过程分析

见解决方法

解决方法

CVE-2020-15778 不受影响,由于堡垒机没有仅开放 scp，不开放 ssh 的场景，因此该漏洞视为不受影响。

CVE-2021-41617 不受影响,堡垒机后台只有一个特权用户，ssh登录后需通过堡垒机console验证才能进入shell。不存在低权用户权限提升的问题。

CVE-2023-38408 不涉及，堡垒机openssh版本为7.4p

CVE-2023-51767 由于实施该攻击需要在堡垒机上存在可以精确读取目标内存临近行内存状态的手段，而该攻击认为是难以实施的（毕竟后台不允许运行无关业务的程序；业务代码则不会有该类特意读取某段内存的逻辑），堡垒机不受影响，也可关闭8022端口规避。

CVE-2018-15919 R6113P03及后续版本不受影响

CVE-2017-15906 R6113P03及后续版本不受影响

CVE-2020-14145 OpenSSH 5.7 到 8.3 版本中，存在算法协商的信息泄露，允许被中间人攻击用于确定攻击目标；由于该泄露需要攻击者控制DNS或者网络流量，因此该漏洞视为不受影响。OpenSSH 允许用户名公钥组合枚举漏洞；由于供应商不认为用户枚举是产品漏洞，且该漏洞不会泄露机密信息，因此该漏洞视为不受影响。

CVE-2018-20685 不涉及,由于堡垒机没有仅开放 scp，不开放 ssh 的场景，因此该漏洞视为不受影响。

CVE-2018-15473 用户枚举漏洞，可关闭8022端口规避。

CVE-2023-48795 可关闭8022端口以及升级R6114P02关闭sshd弱算法规避

CVE-2019-6111 不涉及,由于堡垒机没有仅开放 scp，不开放 ssh 的场景，因此该漏洞视为不受影响

CVE-2019-6109不涉及,由于堡垒机没有仅开放 scp，不开放 ssh 的场景，因此该漏洞视为不受影响