

知

ACG1000是否涉及CVE-2023-48795:SSH协议前缀截断攻击(Terrapin攻击)漏洞

漏洞扫描

卢鹏

2024-05-28 发表

漏洞相关信息

漏洞编号： CVE-2023-48795
漏洞名称： SSH协议前缀截断攻击(Terrapin攻击)漏洞
产品型号及版本： ACG1000

漏洞描述

实施协议扩展以挫败 Fabian Baumer、Marcus Brinkmann 和 Jörg Schwenk 发现的所谓“Terapin 攻击”。这种攻击允许中间人 (adversary-in-the-middle,MITM)在加密开始前发送额外信息，并在加密开始后立即删除相同数量的连续信息，从而有限度地破坏早期加密 SSH 传输协议的完整性。对等 SSH 客户端/服务器将无法检测到信息已被删除。While crvptoaraphically novel. the securty impact of this attack is tortunately very limited as it only allows deetion of consecutve messages, and deleting most messages at this stage of the protocol9 prevents user user authentication from proceeding and results in a stuck connection.

漏洞解决方案

升级R6616P03及以上版本解决