

知 统一数字底盘及SeerEngine-DC不涉及Apache ZooKeeper身份验证绕过漏洞 (CVE-2024-51504)

统一数字底盘 SeerEngine-DC 田毓磊 2024-11-11 发表

漏洞相关信息

漏洞编号: CVE-2024-51504

漏洞名称: Apache ZooKeeper身份验证绕过漏洞

产品型号及版本: 统一数字底盘 E0613H05、SeerEngine-DC E6109

漏洞描述

Apache ZooKeeper是一个分布式协调服务，主要用于管理大型分布式系统中的数据和状态，它提供了高效的分布式锁、配置管理、命名服务和集群管理功能，通过简单的接口支持分布式应用实现一致性和协调。Apache ZooKeeper 3.9.0 - 3.9.3之前版本中存在身份验证绕过漏洞 (CVE-2024-51504)，当ZooKeeper Admin Server使用基于IP的身份验证 (IPAuthenticationProvider) 时，由于默认配置下使用了可被轻易伪造的HTTP请求头 (如X-Forwarded-For) 来检测客户端IP地址，攻击者可通过伪造请求头中的IP地址来绕过身份验证，进而实现未授权访问管理服务器功能并任意执行管理服务器命令 (例如快照和恢复)，从而可能导致信息泄露或服务可用性问题。

影响范围: 3.9.0 <= Apache ZooKeeper < 3.9.3

漏洞解决方案

统一数字底盘及SeerEngine-DC不涉及Apache ZooKeeper身份验证绕过漏洞 (CVE-2024-51504)