SNA Center不涉及Linux systemd中的拒绝服务漏洞

SNA Center 田毓磊 2021-07-24 发表

漏洞相关信息

漏洞编号： CVE-2021-33910
漏洞名称： Linux systemd中的拒绝服务漏洞
产品型号及版本： SNA Center E1209

漏洞描述

漏洞描述：

7月20日， Qualys 研究团队在 systemd 中发现了一个堆栈耗尽拒绝服务漏洞，这是一种在主要 Linux 操作系统上几乎无处不在的实用程序。任何非特权用户都可以利用此漏洞使 systemd 崩溃，从而使整个操作系统崩溃（内核崩溃）。

systemd 是包含在大多数基于 Linux 的操作系统中的软件套件。它为 Linux 操作系统提供了一系列系统组件。它提供了一个系统和服务管理器，作为 PID1运行并启动系统的其余部分。

该漏洞由 systemd v220（2015 年 4 月）的 commit 7410616c（“核心：返工单元名称验证和操作逻辑”）引入，该漏洞将堆中的 strdup() 替换为堆栈中的 strdupa()。成功利用此漏洞允许任何非特权用户造成拒绝服务攻击。

CVE-2021-33909 和 CVE-2021-33910两个漏洞密切相关。

影响范围：

2015 年 4 月以后的所有 systemd 版本都存在漏洞。

漏洞解决方案

SNA Center不涉及Linux systemd中的拒绝服务漏洞。