

知 SNA Center不涉及Linux eBPF本地提权漏洞

SNA Center

田毓磊

2021-08-06 发表

漏洞相关信息

漏洞编号： CVE-2021-3490

漏洞名称： Linux eBPF本地提权漏洞

产品型号及版本： SNA Center E1209

漏洞描述

漏洞描述：

研究人员在 Ubuntu 上的 Linux 内核 eBPF 中发布了针对高危提权漏洞的利用代码，本地攻击者利用该漏洞在 Ubuntu 机器上可以获得root权限。

一位国外安全研究人员发布了 Linux 内核 eBPF（扩展伯克利数据包过滤器）中一个高危漏洞的利用代码，攻击者利用该漏洞可以获得Root权限。

eBPF是一种内核技术（从 Linux 4.x 开始），它允许程序运行而无需更改内核源代码或添加其他模块。它是 Linux 内核中的一种轻量级沙盒虚拟机(VM)，程序员可以在其中运行利用特定内核资源的 BP F 字节码。

安全研究员Valentina Palmiotti发表了一篇博客文章，其中包含有关该漏洞的技术细节以及适用于 Ubuntu 20.10 和 21.04 全新安装的漏洞利用代码。

研究人员还演示了如何利用该问题触发提升权限的 DoS 条件。

影响范围：

linux内核版本： 5.10至5.10.37

linux内核版本： 5.11至5.11.21

linux内核版本： 5.12至5.12.4

linux内核版本： 5.13、 5.13rc1、 5.13rc2、 5.13rc3

漏洞解决方案

SNA Center不涉及Linux eBPF本地提权漏洞。

