کشف چندین آسیب پذیری ممانعت از سرویس در زیرسیستم های USB هسته لینوکس

چندین آسیب‌پذیری در گرداننده[1]های USB لینوکس که شامل زیرسیستم USB هسته لینوکس هستند، یافت شده است. این آسیب‌پذیری‌ها می توانند توسط مهاجمی که دارای دسترسی فیزیکی به دستگاه است، مورد بهره‌برداری قرار گیرند.

این آسیب‌پذیری‌ها به مهاجمان اجازه می دهند در صورت وجود دسترسی فیزیکی، حملات تکذیب سرویس و یا اسکریپت‌های مخرب را بر روی دستگاه اجرا نمایند. به علاوه می‌توانند نسبت به افزایش سطح دسترسی اقدام نمایند.

تمامی آسیب‌پذیری‌ها توسط یکی از کارشناسان امنیتی گوگل کشف شده و به انجمن لینوکس گزارش شده است. کارشناس مذکور ۷۹ اشکال هسته لینوکس را پیدا کرده و تا کنون تنها ۱۴ مورد از آنها را گزارش نموده است.

---

[1] Driver

CVEها – USB لینوکس

با توجه به گزارش‌های واصله، در زیر جزئیات ۱۴ آسیب‌پذیری که توسط syzkaller در زیرسیستم USB هسته لینوکس کشف شده، آمده است. همه این آسیب‌پذیری‌ها می‌توانند توسط یک دستگاه USB مخرب جعلی - در صورت دسترسی فیزیکی مهاجم به دستگاه - ، مورد بهره‌برداری قرار گیرند.

CVE-2017-16525

CVE-2017-16526

CVE-2017-16527

CVE-2017-16528

CVE-2017-16529

CVE-2017-16530

CVE-2017-16531

CVE-2017-16532

CVE-2017-16533

CVE-2017-16534

CVE-2017-16535

CVE-2017-16536

CVE-2017-16537

CVE-2017-16538

این آسیب‌پذیری‌ها با استفاده از syzkaller کشف شده‌اند. syzkaller از ابزارهای فازینگ گوگل است و از akaros، freebsd، fuchsia، netbsd و windows پشتیبانی می‌نماید.

Syzkaller یک از کارافتادگی[۲] هسته‌ی سیستم عامل را تشخیص می‌دهد و به طور خودکار روند بازتولید این از کار افتادگی را آغاز می‌کند. در انتها برنامه‌ی ایجادکننده‌ی از کارافتادگی را به حالت کمینه می رساند که بخش آسیب‌پذیر به راحتی قابل تشخیص باشد.

ابزار امن‌سازی لینوکس

Lynis یک ابزار متن‌باز جهت ممیزی امنیت در سیستم‌عامل‌های مبتنی بر یونیکس و لینوکس است. این ابزار با چک کردن تعداد زیادی از کنترل‌های امنیتی، سیستم را پویش می‌کند. پس از پویش، گزارشِ تمامِ یافته‌ها نمایش داده خواهد شد.

محققان دانشگاه لندن ابزار POTUS را ارائه داده‌اند که به طور خودکار آسیب‌پذیری‌ها را در گرداننده های دستگاه USB سیستم لینوکس پیدا می‌کند. این ابزار قادر به شناسایی آسیب‌پذیری روز صفر نیز میباشد. آنها دو مورد از آسیب‌پذیری‌های روز صفر کشف نشده را در هسته اصلی لینوکس و به وسیله ابزار POTUS پیدا کرده و تایید نموده‌اند.

منبع خبر: gbhackers.com

لینک خبر: https://gbhackers.com/multiple-denial-service-linux-usb/

---

۲ Crash