آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه الکترونیکی تحلیل رویدادهای امنیت سایبری (روزانه)

یکشنبه ۲۲ اسفند ۱۴۰۰

کشف آسیب پذیری «Dirty Pipe» در کرنل لینوکس

نسخه ۱,۰,۰

آسیب‌پذیری "Dirty Pipe" در هسته سیستم‌عامل لینوکس طیف مختلفی از دستگاه‌ها را تحت تأثیر قرار می‌دهد

تاریخ: ۱۴/ مارس / ۲۰۲۲

بررسی اجمالی:

یک محقق امنیت سایبری به نام Max Kellermann در شرکت میزبانی وب IONOS اخیراً در مورد یک آسیب‌پذیری امنیتی در هسته سیستم‌عامل لینوکس هشدار داده است. مهاجمان سایبری با سوءاستفاده از این نقص امنیتی می‌توانند با افزایش سطح دسترسی حتی کنترل دستگاه آسیب‌پذیر را به دست‌گیرند [۲,۱].

نگاه کلی:

عنوان	توضیحات
دستگاه‌های آسیب‌پذیر	کرنل‌های لینوکس قبل از نسخه ۵,۱۶,۱۱ و ۵,۱۵,۲۵ و ۵,۱۰,۱۰۲
راه‌های نفوذ	نوشتن داده‌های اختیاری بر روی فایل‌های فقط خواندنی از طریق pipe
هدف مهاجمان	افزایش سطح دسترسی و در اختیار گرفتن سیستم هدف به‌طور کامل
شناسه آسیب‌پذیری	CVE-2022-0847
شدت خطر	نمره ۷,۸ از ۱۰ در استاندارد CVSS

توضیحات بیشتر:

به گفته Max Kellermann یک آسیب‌پذیری Dirty Pipe باقابلیت افزایش سطح دسترسی و حتی تزریق کدهای مخرب در هسته سیستم‌عامل لینوکس وجود دارد. این نقص امنیتی کرنل‌های لینوکس قبل از نسخه ۵,۱۶,۱۱ و ۵,۱۵,۲۵ و ۵,۱۰,۱۰۲ را تحت تأثیر قرار داده و حتی می‌تواند کنترل دستگاه آسیب‌پذیر را در اختیار مهاجمان سایبری قرار دهد [۲,۱].

نقص امنیتی مذکور با شناسه CVE-2022-0847 و امتیاز ۷٫۸ از ۱۰ در استاندارد CVSS نوعی مشکل مربوط به مدیریت حافظه است که قابلیت نگارش داده‌های دلخواه در فایل‌های فقط خواندنی را فراهم می‌سازد. امری که از طریق آن حتی قابلیت کنترل دستگاه‌های آسیب‌پذیر نیز ممکن خواهد شد [۲,۱].

محققان شرکت کسپرسکی در رابطه با این آسیب‌پذیری می‌گویند : یک کاربر محلی غیرمجاز می‌تواند از نقص امنیتی Dirty Pipe برای نوشتن صفحات موجود در حافظه پنهان سیستم‌عامل (صفحات فقط خواندنی) استفاده کنند. امری که به علت مقداردهی نادرست ابتدایی ساختار حافظه بافر Pipe هنگام ایجاد آن رخ خواهد داد. درواقع متغیر flag در توابع copy_page_to_iter_pipe و push_pipe مقداردهی اولیه درستی نداشته‌اند [۲,۱].

Pipe یا خط لوله یک مکانیسم ارتباطی بین فرآیندی یک‌طرفه بوده که در آن مجموعه‌ای از فرآیندها به‌صورت زنجیره‌ای به هم متصل می‌شوند. در Pipe هر فرآیند ورودی را از فرآیند قبلی گرفته و خروجی را برای فرآیند بعدی تولید می‌کند [۳].

قابلیت تنظیم کارها به کمک سیستم Cron نیز در سیستم‌عامل با سوءاستفاده از این آسیب‌پذیری ممکن است. علاوه بر این قابلیت تغییر فایل‌های حساسی نظیر /etc/passwd و همچنین تخریب Containerها هم وجود دارد. لازم به ذکر است که مشکل CVE-2022-0847 در نسخه‌های لینوکس ۵,۱۶,۱۱، ۵,۱۵,۲۵ و ۵,۱۰,۱۰۲ سه روز پس از گزارش آن به تیم امنیتی هسته لینوکس، برطرف گردید. برای سایر نسخه‌ها نیز در حال حاضر هیچ‌گونه اقدام کاهشی وجود نداشته و باید منتظر به‌روزرسانی‌های امنیتی مربوطه بود [۲,۱].

منابع:

1. The Hacker News Website
2. ThreatPost Website
3. The Hacker News Website