禪

بازهم یک آسیبپذیری خطرناک دیگر

شناسایی حفرهای خطرناک در دوربینهای وایفای دیلینک

محصولات شرکت دیلینک به ویژه دوربینهای این شرکت از جمله محصولات پر فروش بازار به شمار میروند . اما به تازگی آسیبپذیری جدید و وصله نشدهای در دوربینهای بیسیم این شرکت شناسایی شده که به هکرها اجازه میدهد گذرواژه مورد استفاده در دوربینها را ریست کرده و از راه دور به تصاویر ارائه شده توسط این دوربینها دسترسی داشته باشند .

این رخنه توسط پژوهشگران استارتآپ امنیتی اینترنت اشیا سنریو در غالب بخشی از تجزیه و تحلیل آنها در ارتباط با آسیبپذیریهای موجود در دستگاههای سازمانی و مصرفی شناسایی شده است . این رخنه روی دوربینهای وای فای دی لینک سری DCS-930L که ویژه خانهها و برای نظرات ویدیویی و تصویری طراحی شده است وجود دارد. حفره امنیتی یک سرریز پشته است که در سرویس پردازش فرمانهای راه دور این دوربینها رخ میدهد. این گروه از کارشناسان امنیتی، حمله خود را تنها روی دوربینهای سری DCS-930L متمرکز کرده بودند . اما بر این باور هستند که این حفره در سایر محصولات این شرکت که از این چنین ساز و کاری استفاده میکنند وجود دارد .

مطلب پیشنهادی

بیگانهای پرسه میزند

مسیریابها و دستگاههای اینترنت اشیا در معرض تهدید بدافزار **Remaiten**

این آسیبپذیری دقیقا چگونه رخ میدهد؟

کارشناسان امنیتی این استارتآپ اعلام داشتهاند که تابع آسیبپذیر، دادههایی را از یک رشته ورودی به یک بافر پشته رونویسی میکند . اینکار باعث بازنویسی دوباره آدرس بازگشتی این تابع میشود . این آسیبپذیری از طریق یک دستورالعل منفرد که شامل کد اسمبلی پیشرفته و یک رشته که برای استفاده از این سرریز طراحی شده، قابل بهرهبرداری است . این تابع در ابتدا کد اسمبلی را در یک آدرس اجرایی ثابتی کپی میکند . در گام بعد، این دستور یک سرریز پشته را تولید کرده و مقدار نشانی بازگشتی تابع را به نشانی کد اسمبلی که توسط هکر طراحی شده است، تغییر میدهد . این آسیبپذیری شرایط را برای پیادهسازی حمله تزریق کد (Code Injection) که برای رونویسی گذرواژه مورد استفاده قرار میگیرد، آماده میکند . سرانجام هکر این توانایی را به دست خواهد آورد تا از راه دور به تصاویر ضبط شده توسط این دوربینها دسترسی پیدا کند .

استارتآپ سنریو اعلام کرده است که این آسیبپذیری را به شرکت دی لینک گزارش کرده و شرکت سازنده در تلاش است تا وصله مربوطه را در اولین زمان ممکن ارائه کند . نکتهای که باعث خطرناکی این آسیبپذیری شده به گفته کارشناسان امنیتی اشاره دارد که میگویند بهرهبرداری از این آسیبپذیری کار چندان پیچیدهای نیست، بدتر آنکه شرکت آمازون این محصول را به عنوان یکی از کالاهای پر فروش و محبوب رتبهبندی کرده و به همین دلیل پیشبینی میشود کاربران زیادی قربانی این آسیبپذیری شوند . در این حمله تمام آن چیزی که یک هکر به آن نیاز دارد ورود به شبکهای است تا بتواند از طریق آن با این دوربینها ارتباط برقرار کند . لازم به توضیح است که تفاوتی نمیکند این یک شبکه محلی یا شبکه جهانی اینترنت باشد . هکر نه تنها به اطلاعات بیشتر حتا به اطلاعات مرتبط به ورودی دستگاه هم نیازی ندارد . این چندمین باری است که یک حفره امنیتی و یک آسیبپذیری جدی در دوربینهای DCS-930L کشف میشود. سال گذشته نیز پژوهشگران خبر از یک حفره آپلود بدون محدودیت فایلها دادند . در ماه ژانویه نیز کارشناسان گزارش کردند هکرها این توانایی را دارند تا این دستگاهها را دوباره برنامهریزی کرده و آنها را تبدیل به یک درب پشتی پایدار کنند . (دوربینهای زامبی)

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
00:13 - 08/04/1395
برچسب:
امنیت - رخنه - دی لینک - آسیب پذیری - دوربین وای فای - تزریق کد - Code Injection

---

□□□□□ منبع: https://www.shabakeh-mag.com/security/3610