خداحافظ RC4

چرا یک الگوی رمزنگاری با قدمتی 30 ساله از مرورگرها حذف می‌شود؟

گوگل، مایکروسافت و موزیلا با آغاز سال نو میلادی پشتیبانی از رمزنگاری RC4 را در مرورگرهای کروم، اینترنت اکسپلورر، ایج و فایرفاکس متوقف می‌کنند. نزدیک به 30 سال است این متد رمزنگاری در مرورگرهای وب مورد استفاده قرار می‌گیرد و رخنه‌ها و آسیب‌پذیری‌های زیادی هم داشته که تا کنون پایه‌گذاری بسیاری از بدافزارها بوده‌اند.

سه شرکت بزرگ دنیای فناوری روز سه‌شنبه اعلام کردند، مرورگرهای کروم، ایج، اینترنت اکسپلورر و فایرفاکس از سال جاری میلادی پشتیبانی از الگوی رمزنگاری RC4 (به اختصار Rivest Cipher 4) را متوقف می‌کنند. RC4 یک رمز دنباله‌ای (stream cipher) است که در سال 1984 طراحی شد و شیوه عملکرداش به گونه‌ای است که عناصر ورودی را به‌طور پیوسته مورد پردازش قرار داده و شبیه به حالت صف عنصر به عنصر یک متن را رمزنگاری می‌کند.

RC4 به‌طور گسترده‌ای توسط مرورگرهای اینترنتی، سرویس‌های آنلاین و برنامه‌های کاربردی مورد استفاده قرار می‌گیرد. آسیب‌پذیری‌های متعددی که چند سال بعد در این فناوری امنیتی شناسایی شد، اولین نشانه‌های غیر قابل اطمینان بودن این فناوری امنیتی را رقم زد. مکانیزم مورد استفاده در این الگوریتم رمزنگاری به‌گونه‌ای است که کار را برای عامل‌های مخرب ساده کرده و باعث می‌شود، سرویس‌هایی که سیاست کاری خود را روی این فناوری متمرکز کرده‌اند، در مدت زمانی بین چند ساعت تا چند روز شکسته شوند. محققان برای آن‌که نشان دهند این رمزنگاری ضعیف بوده و به راحتی شکسته می‌شود، توانستند آن‌را ظرف مدت چند ساعت هک کنند.

در اوایل سال جاری میلادی، آسیب‌پذیری جدیدی بر مبنای الگوریتم RC4 روی ارتباطات SSL/TLS شناسایی شد. بررسی‌های اولیه نشان دادند که آسیب‌پذیری موجود در RC4 باعث می‌شود تا هکرها به آسانی پروتکل‌های امنیتی SSL و TLS را مورد حمله قرار دهند. در فوریه سال جاری، سازمان IETF (به اختصار Internet Engineering Task Force) اعلام کرد کلاینت‌های TLS در زمان ایجاد و برقراری یک ارتباط، هرگز نباید از RC4 استفاده کنند. مرورگرها باید کاملا اطمینان حاصل کنند فقط در مواقع ضروری نیازمند Cipher های RC4 هستند و در شرایط دیگر نباید اقدام به استفاده از RC4 کنند. با این حال، سه شرکت بزرگ که محبوب‌ترین مرورگرهای اینترنتی را در اختیار دارند اعلام کرده‌اند پشتیبانی از RC4 را به‌طور کامل در نسخه‌های بعدی مرورگرهای‌شان غیر فعال خواهند کرد.

مایکروسافت تا سه ماه دیگر RC4 را بازنشسته می‌کند

مایکروسافت با آغاز سال 2016 میلادی به‌طور پیش‌فرض پشتیبانی از RC4 را در مرورگرهای اینترنت اکسپلورر و ایج غیر فعال خواهد کرد. این شرکت به مالکان وب سرویس‌هایی که هنوز هم وابستگی زیادی به این فناوری رمزنگاری دارند اعلام کرده است برای پیشگیری از بروز مشکلاتی که در آینده آن‌ها را تهدید می‌کند، به دنبال جایگزین‌های مناسبی برای RC4 باشند.

گوگل آماده گذر از RC4 است

گوگل هم رویکرد مشابهی را در ارتباط با غیر فعال کردن RC4 در نسخه بعدی مرورگر خود نظر گرفته است. اما در گزارش‌های منتشر شده تاریخ دقیقی در این زمینه اعلام نشده است. آدام لانجلی از کارمندان گوگل در این خصوص اعلام کرده است، برآوردها نشان می‌دهد فقط 0.13 درصد از کاربران مرورگر کروم که از ارتباطات HTTPS استفاده می‌کنند به RC4 وابسته هستند. در سمت سرور، اپراتورهای سرور به احتمال بسیار زیاد این توانایی را دارند تا به پیکربندی یک بسته cipher مناسب‌تری نسبت به RC4 اقدام کنند. این کار باعث می‌شود تا آن‌ها با ضریب اطمینان بالاتری به فعالیت‌های خود به پردازند.» لانجلی در ادامه صحبت‌های خود افزود: «حذف کامل RC4 به احتمال زیاد وضعیت پایدارتری در کانال‌های ارتباطی به وجود خواهد آورد. دستاوردهای این رویکرد از ژانویه یا فوریه سال 2016 میلادی خود را نشان خواهند داد. در آن زمان سرورهای HTTPS که تنها از الگوریتم RC4 استفاده می‌کنند از کار کردن باز خواهند ماند.»

موزیلا تاریخ دقیقی اعلام کرد

موزیلا، تنها شرکتی است که تاریخ دقیق حذف این رمزنگاری را اعلام کرده است. موزیلا در نظر دارد با عرضه فایرفاکس نسخه 44 پشتیبانی از این الگوریتم را به‌طور کامل متوقف سازد. موزیلا در نظر دارد فایرفاکس 44 را در ژانویه 2016 میلادی در اختیار کاربران قرار دهد. بنابر گزارش بنیاد موزیلا نزدیک به 0.08 درصد کاربران فایرفاکس از RC4 استفاده می‌کنند.

منبع:

wccftech

تاریخ انتشار:
28 شهریور 1394

نشانی منبع: https://www.shabakeh-mag.com/security/1606