سرعت انتشار وصله‌ها بیش‌تر شده است

رشد حملات Zero-Day و شکاف‌های امنیتی مرورگرها

شرکت امنیتی Secunia طی گزارشی وضعیت انواع آسیب‌پذیری‌ها و وصله‌های منتشر شده برای آن‌ها را در سال 2014 اعلام کرد. جالب است که شکاف‌های امنیتی روز صفر یا Zero-Day و مرورگرهای وب بیش‌تر شده، ولی از سوی دیگر سرعت انتشار وصله‌های امنیتی شرکت‌ها نیز افزایش یافته است.

آسیب‌پذیری‌های روز صفر که به‌طور عمده نقص‌های امنیتی در نرم‌افزارها هستند، توسط هکرها مورد استفاده قرار گرفته و به‌طور عمومی نیز اطلاع‌رسانی شده‌اند که از 14 درصد در سال 2013 به 25 درصد در سال 2014 رسیده‌اند. برخی از این شکاف‌های امنیتی بسیار خطرناک و حیاتی هستند و هنوز برای آن‌ها وصله یا بسته به‌روزرسانی منتشر نشده و احتمال استفاده توسط هکرها زیاد است. آسیب‌پذیری‌های مرورگرهای وب نیز از 728 عدد به 1035 عدد در سال 2014 رسیده است. خبر خوب این است که شرکت‌های توسعه‌دهنده نرم‌افزارها سرعت انتشار وصله‌ها را افزایش دادند. Secunia می‌گوید برای 83 درصد از 15435 آسیب‌پذیری که در 3870 برنامه کاربردی شناسایی کرده است، وصله‌های امنیتی منتشر و رفع نقص شده‌اند. البته در این آمار و ارقام، آسیب‌پذیری‌هایی که به‌طور عمومی فاش شدند مدنظر است. در سال 2013، برای 78.5 درصد آسیب‌پذیری‌های عمومی وصله امنیتی منتشر شده بود. در سال 2009، این رقم 49.9 درصد بود. این گزارش نشان می‌دهد شرکت‌ها نسبت به آسیب‌پذیری‌ها سریع‌تر و هشیارتر واکنش نشان می‌دهند و شکاف‌های امنیتی را جدی می‌گیرند.
احتمال دیگری نیز وجود دارد. در سال‌های اخیر، محققان امنیتی با شرکت‌های توسعه‌دهنده نرم‌افزارها و آزمایشگاه‌های فنی این شرکت‌ها ارتباطات بهتر و بیش‌تری برقرار کرده‌اند و گزارش‌های کشف شکاف‌های امنیتی را سریع‌تر و حتی مخفیانه به دست شرکت‌ها می‌رسانند. در نتیجه، شرکت‌ها وصله‌های امنیتی را سریع‌تر آماده و منتشر می‌کنند. گزارش نتیجه دیگری هم دارد. اگر شرکت‌ها در همان روزهای اولیه شناسایی آسیب‌پذیری وصله امنیتی را منتشر نکنند، احتمالاً دیگر منتشر نخواهند کرد و برنامه‌ای برای رفع نقص نرم‌افزارشان ندارند. درصد نرم‌افزارهایی که وصله امنیتی یک ماه بعد از مشخص شدن شکاف امنیتی وجود داشته است، برابر 84.3 است. طبق این گزارش، در نرم‌افزار پی‌دی‌اف که هدف بزرگی برای هکرها است و به‌طور متناوب مورد حمله قرار می‌گیرد و تقریباً روی هر کامپیوتر نصب شده است (با سهم بازار 85 درصدی)، 43 شکاف امنیتی وجود دارد. در سال‌های اخیر، ادوبی ابزارها و برنامه‌های بسیار قدرتمندی برای اسکن برنامه‌ها و کدهای امنیتی در جهت یافتن مشکلات، شکاف‌ها و تولید سریع وصله‌ها در هنگام شناسایی آسیب‌پذیری طراحی کرده است. به همین دلیل، تنها 32 درصد کامپیوترهایی که به نرم‌افزارهای ادوبی مجهز هستند، هنوز وصله‌های جدید را نصب نکرده یا برنامه‌ها را به‌روزرسانی نکرده‌اند و در معرض خطر قرار دارند. Secunia درباره آسیب‌پذیری‌های نرم‌افزارهای منبع باز پس از کشف چند شکاف امنیتی در سیستم رمزنگاری OpenSSL در سال گذشته، نگران‌های جدی دارد و وضعیت آن‌ها را نیز مورد تحقیق و بررسی

قرار داده است. شکاف امنیتی Heartbleed در رمزنگاری OpenSSL در سال 2014 سروصدای بسیار زیادی به‌راه انداخت؛ زیرا طیف بزرگی از نرم‌افزارها و وب‌سایت‌ها این آسیب‌پذیری را دارند. با این شرایط، به‌نظر می‌رسید شرکت‌ها و توسعه‌دهندگان نرم‌افزارها به‌سرعت وصله‌های امنیتی را منتشر کرده‌اند، اما مطالعه اخیر Secunia نشان می‌دهد این طور نیست و هنوز بسیاری از شرکت‌ها برای OpenSSL وصله امنیتی نداده‌اند یا خیلی با تأخیر اقدام کرده‌اند. این مؤسسه امنیتی درباره نرم‌افزارهای منبع باز می‌گوید: «شرکت‌ها نباید فقط به به‌روزرسانی‌های دوره‌ای درباره نرم‌افزارهای منبع باز بسنده کنند و در مقابل یک شکاف امنیتی که کشف و آشکار شده است، سریع‌تر واکنش نشان دهند.»

تاریخ انتشار:

30 اردیبهشت 1394

نشانی منبع: https://www.shabakeh-mag.com/security/655