کد خبر: ۱۰۰۲۷۵۲
شنبه ۳۱ فروردین ۱۳۹۸ ۱۶:۴۸

انتشار بروزرسانی امنیتی جدید شرکت ادوبی

شرکت ادوبی وصله بروزرسانی امنیتی بزرگی برای چندین نرم‌افزار ارائه‌شده خود منتشر ساخته است که تعدادی از اشکالات مهم و بحرانی را برطرف می‌سازد.

به گزارش گروه علم وفناوری ایسکانیوز، ادوبی در بولتن امنیتی ماه آوریل سال ۲۰۱۹ خود یک بروزرسانی برای تقویت امنیت ، ، ، ، ، و لیست کرده است.
برخی از آسیب‌پذیری‌های برطرف‌شده می‌توانند منجر به مشکلات اجرای کد دلخواه، افشای اطلاعات حساس و اجرای کد راه‌دور در متن کاربر فعلی شوند.

در ، یک خطای سرریز پشته با شناسه۷۱۳۰-۲۰۱۹- که می‌توانست منجر به اجرای کد راه دور شود به همراه یک نقص نوشتن خارج از محدوده (---) با شناسه‌ی ۷۱۳۲-۲۰۱۹- که می‌تواند با همان هدف مورد سواستفاده قرار گیرد، وصله شده است. این به‌روزرسانی امنیتی، شش خطای افشای اطلاعات را نیز در این نرم‌افزار برطرف می‌سازد.

ادوبی آسیب‌پذیری اسکریپت‌نویسی متقابل () با شناسه۷۱۲۹-۲۰۱۹- را در برطرف ساخته است که اگر توسط مهاجم مورد سواستفاده قرار گیرد، ممکن است منجر به نشت اطلاعات حساس شود.

در آسیب‌پذیری با شناسه۷۱۰۷-۲۰۱۹- وصله شده است. این اشکال بحرانی ناشی از پردازش ناامنی است که می‌تواند منجر به اجرای کد دلخواه در متن کاربر فعلی شود. دو آسیب‌پذیری ۷۱۰۵-۲۰۱۹- و ۷۱۰۶-۲۰۱۹- نیز در وصله شده‌اند که سواستفاده از آن‌ها می‌تواند منجر به اجرای کد دلخواه شود.

در مجموع هفت آسیب‌پذیری امنیتی جدی در آخرین وصله‌ی به‌روزرسانی امنیتی ادوبی برای برطرف شده است. این اشکالات (-۲۰۱۹-۷۱۰۳، -۲۰۱۹-۷۱۰۲، -۲۰۱۹-۷۱۰۱، -۲۰۱۹-۷۱۰۰، -۲۰۱۹-۷۰۹۹، -۲۰۱۹-۷۰۹۸ و -۲۰۱۹-۷۱۰۴) همگی مسائل مربوط به خرابی حافظه هستند که می‌توانند به منظور اجرای کد دلخواه مورد سواستفاده قرار گیرند.

یک جفت آسیب پذیری مهم و حیاتی با شناسه‌های ۷۱۰۸-۲۰۱۹- و ۷۰۹۶-۲۰۱۹- در رفع شده است. این نقص‌های خواندن خارج از محدوده و استفاده پس از آزادسازی (--) می‌توانند منجر به نشت اطلاعات یا استفاده از کد دلخواه شوند.
به‌روزرسانی قابل‌توجهی در وصله ماه آوریل ادوبی دریافت کرده است. در مجموع، ۲۱ مسئله برطرف شده است که ۱۰ مورد از آن‌ها می‌تواند منجر به افشای اطلاعات شود و ۱۱ اشکال می‌تواند به منظور اجرای کد دلخواه مورد سواستفاده قرار گیرد.

یک نقص امنیتی متوسط با شناسه۷۰۹۷-۲۰۱۹- نیز را تحت تأثیر قرار داده است. اگر پروتکل‌های انسداد پیامک کارگزار () نهاد رله‌سازی حملات در این نرم‌افزار باشند، این نقص می‌تواند برای نشت اطلاعات حساس مورد سواستفاده قرار گیرد.
توصیه می‌شود کاربران بروزرسانی‌های خودکار را به منظور کاهش خطرات سواستفاده دریافت کنند.

انتهای پیام/