بولتن خبری هفتگی کاشف شماره ۶۶-۶۵

خبرها، هشدارها و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات

تاریخ انتشار: ۹۷/۱۲/۲۸

توجه: در این بولتن، مهمترین خبرها، هشدارها و آسیب‌پذیری‌های حوزه امنیت فضای تولید و تبادل اطلاعات در هفت روز گذشته که بر اساس متدولوژی داخلی شرکت کاشف از منابع متنوع، استخراج شده است، به‌منظور یادآوری به ذی‌نفعان، منتشر می‌شود. لذا بدینوسیله توصیه می‌شود که بانک‌ها و مؤسسات مالی، استفاده از این بولتن خبری را درکنار فرآیندهای داخلی پایش و رصد اخبار و آسیب‌پذیری‌های مربوط به محصولات مورد استفادهٔ خویش، در نظر داشته باشند.

آسیب‌پذیری‌ها

اهم آسیب‌پذیری‌های هفت روز گذشته در جدول زیر ارائه شده است:

محصول	شرح	منبع
آسیب‌پذیری	میلیون‌ها سایت وردپرسی در معرض آسیب‌پذیری اجرای کد	Link

هشدارها!

هشدارهای منتشر شده از سوی شرکت کاشف در طی چند روز گذشته در جدول زیر ارائه شده است:

شماره هشدار	تاریخ انتشار	عنوان	فایل ارسال شده
Alert-۹۷۱۰۰	۲۱ اسفند ۱۳۹۷	بروزرسانی‌های امنیتی سیسکو	Alert-۹۷۱۰۰
Alert-۹۷۱۰۱	۲۱ اسفند ۱۳۹۷	افشای آسیب‌پذیری روز صفر در macOS	Alert-۹۷۱۰۱
Alert-۹۷۱۰۲	۲۱ اسفند ۱۳۹۷	انتشار وصله امنیتی برای آسیب‌پذیری روز صفر ColdFusion	Alert-۹۷۱۰۲
Alert-۹۷۱۰۳	۲۸ اسفند ۱۳۹۷	نفوذ به Windows Server از طریق باگ سرویس WDS	Alert-۹۷۱۰۳
Alert-۹۷۱۰۴	۲۸ اسفند ۱۳۹۷	میلیون‌ها سایت وردپرسی در معرض آسیب‌پذیری اجرای کد	Alert-۹۷۱۰۴
۹۷۱۱۴	۲۱ اسفند ۱۳۹۷	مرورگر کروم را به آخرین وصله های امنیتی بروزرسانی کنید	۹۷۱۱۴
۹۷۱۱۵	۲۸ اسفند ۱۳۹۷	به‌روزرسانی‌های امنیتی Photoshop و Digital Editions Adobe	۹۷۱۱۵

خبرها

اهم خبرهای چند روز گذشته در جدول زیر ارائه شده است:

شماره	عنوان و لینک خبر
۱	گوگل Backstory را منتشر کرد
۲	استفاده دوباره هکرها از باگ Equation Editor در آفیس
۳	سرویس انتقال فایل رایگان رمزگذاری شده فایرفاکس
۴	مایکروسافت وصله‌هایی را برای ۶۴ نقص منتشر کرد
۵	نشت ۸۰۰ میلیون داده از یک پایگاه‌داده ناامن
۶	بدافزار StealthWorker
۷	استفاده بدافزار SLUB از گیت هاب و اسلک برای کانال ارتباطی
۸	دستگاه‌های با UPnP اصلاح نشده در معرض حملات هستند
۹	گسترش باج‌افزار Yatron از طریق اکسپلویت EternalBlue
۱۰	انتشار یک ابزار مهندسی معکوس قدرتمند با نام GHIDRA ۹,۰
۱۱	کشف یک آسیب‌پذیری روز صفر جدید در کروم
۱۲	حمله به سامانه های ویندوزی با بدافزارFarseer
۱۳	افشای یک نقص وصله نشده در کرنلmacOS
۱۴	تکامل باتنتNecurs
۱۵	رفع نقص‌های DoS و اجرای کد از راه دور درRSLinx Software
۱۶	حفره امنیتی Spoiler در پردازنده‌های اینتل