خبرنامه‌ی تخصصی امنیت

هفته‌نامه‌ی شماره ۱۷ ، اسفند ۹۹ ، سال اول
مرکز تخصصی آپا ـ دانشگاه ارومیه

آنچه در این شماره ارائه شده:

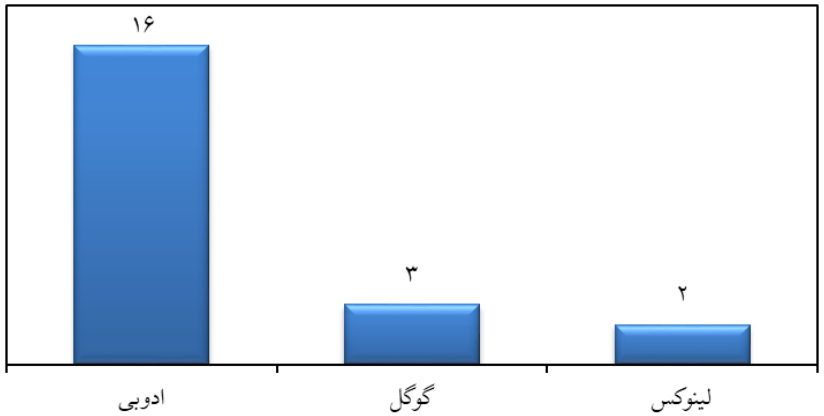
- مروری بر آسیب‌پذیری‌های مهم هفته
- آسیب‌پذیری‌های مهم در محصولات شرکت ادوبی
- خبرهای مهم امنیتی این هفته

بسم الله الرحمن الرحيم

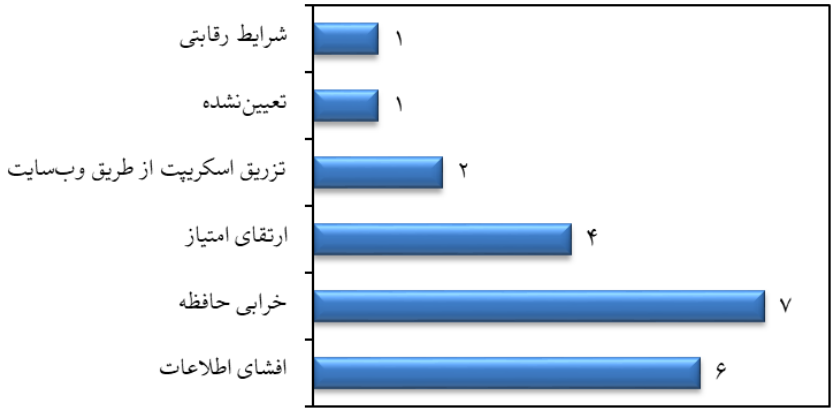
مروری بر آسیب‌پذیری‌های مهم در هفته‌ی چهارم اسفند ۹۹

در هفته‌ای که گذشت، در مجموع ۲۱ آسیب‌پذیری در محصولات شرکت‌های مختلف شناسایی شدند. در میان شرکت‌های مختلف، ادوبی بیشترین محصولات آسیب‌پذیر را به خود اختصاص داده است. بیشتر این آسیب‌پذیری‌ها از نوع خرابی حافظه هستند. در ادامه، سایر آمار و اطلاعات مربوط به این آسیب‌پذیری‌ها ارائه شده است.

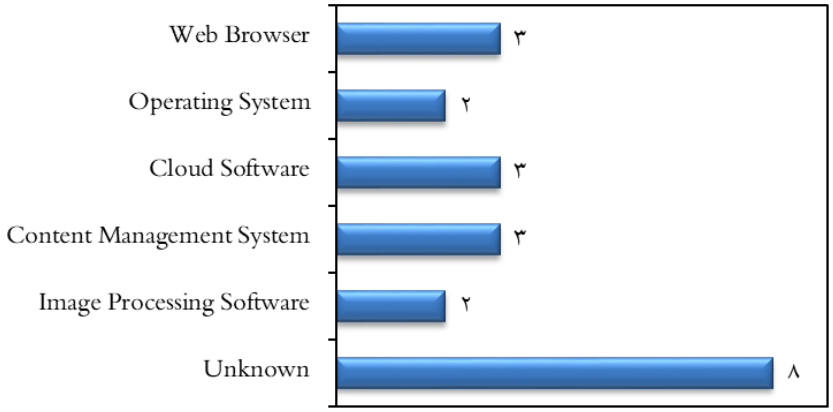
تعداد آسیب‌پذیری‌ها به تفکیک شرکت سازنده



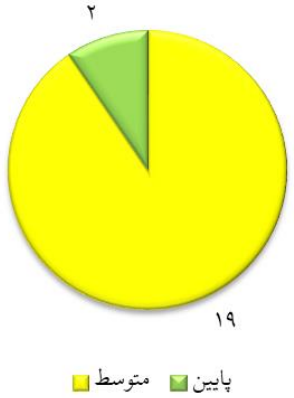
انواع آسیب‌پذیری‌ها



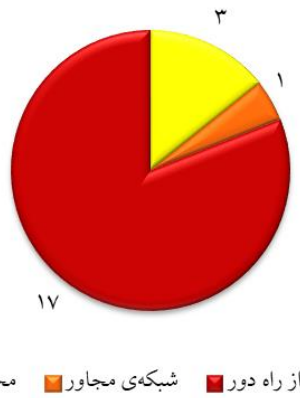
انواع محصولات آسیب‌پذیر



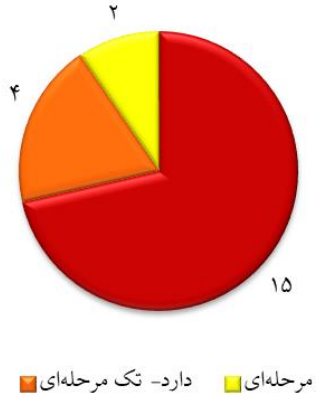
سطح خطر آسیب‌پذیری‌ها



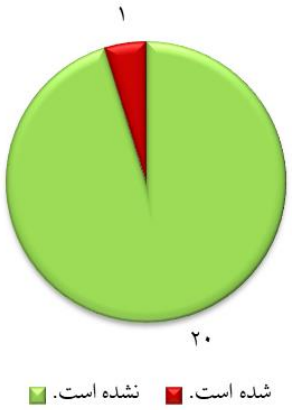
بردار دسترسی آسیب‌پذیری‌ها



نیاز به احراز هویت برای بهره‌برداری از آسیب‌پذیری‌ها



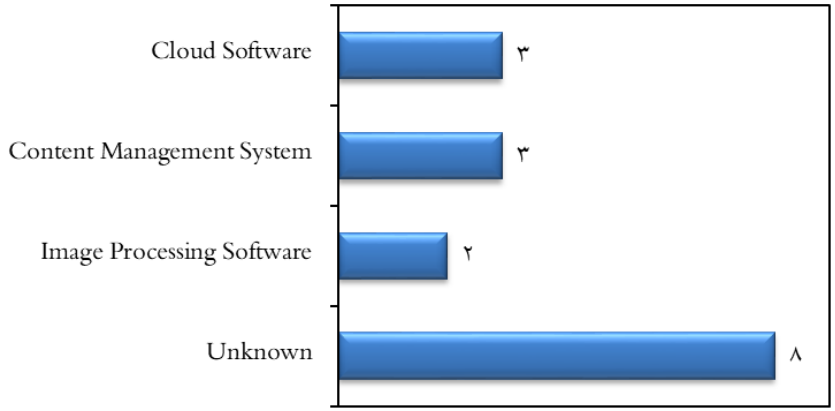
وضعیت بهره‌برداری از آسیب‌پذیری‌ها



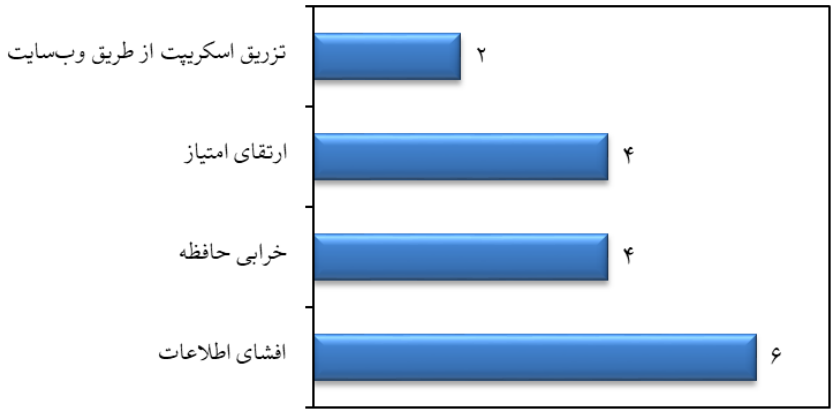
آسیب‌پذیری‌های شناسایی‌شده در محصولات شرکت ادوبی

در هفته‌ای که گذشت، در مجموع ۱۶ آسیب‌پذیری در محصولات مختلف ادوبی شناسایی شدند. در ادامه، آمار و اطلاعات مربوط به این آسیب‌پذیری‌ها ارائه شده است.

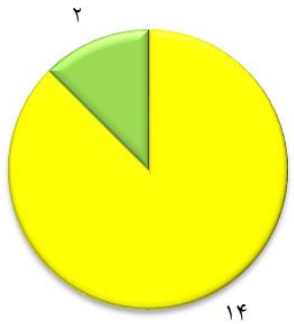
انواع محصولات آسیب‌پذیر



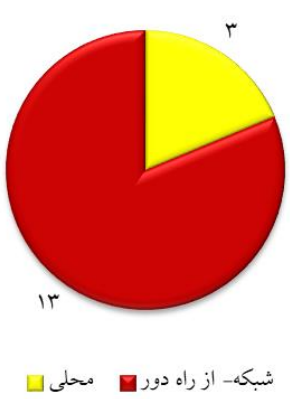
انواع آسیب‌پذیری‌ها



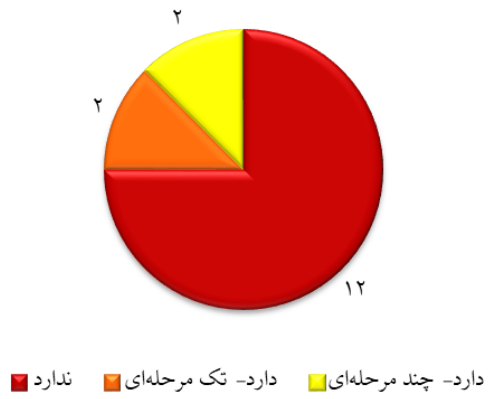
سطح خطر آسیب‌پذیری‌ها



بردار دسترسی آسیب‌پذیری‌ها



نیاز به احراز هویت برای بهره‌برداری از آسیب‌پذیری‌ها



خبرهای مهم امنیتی در هفته‌ی چهارم اسفند ۹۹

۲۲ اسفند

کد اثبات مفهومی آسیب‌پذیری‌های ProxyLogon منتشر شده است!

با وجود تلاش‌های مایکروسافت برای کاهش بهره‌برداری‌ها، اولین بهره‌برداری اثبات مفهومی عمومی کاربردی برای آسیب‌پذیری‌های ProxyLogon منتشر شده است.
علاوه‌براین، یک گزارش فنی دقیق نیز توسط محققانی که مهندسی معکوس CVE-2021-26855 را انجام داده‌اند، منتشر شده است. در این گزارش، علاوه‌بر اطلاعات فنی، با شناسایی تفاوت بین نسخه‌های آسیب‌پذیر و وصله‌شده، یک بهره‌برداری کاملاً کارامد end-to-end نیز ارائه شده است.

۲۲ اسفند

سرورهای Exchange مایکروسافت هدف حمله‌ی باج‌افزاری قرار گرفته‌اند!

مجرمان سایبری آسیب‌پذیری‌های ProxyLogon شناسایی شده در سرورهای Exchange مایکروسافت را با هدف نصب یک باج‌افزار جدید به نام DearCry مورد بهره‌برداری قرار داده‌اند.
به گفته محققان، مایکروسافت نوع جدیدی از حملات باج‌افزاری را شناسایی کرده است که Ransom:Win32/DoejoCrypt.A نام دارد. این حملات باج‌افزاری به مدیریت نیروی انسانی هم‌اکنون در حال بهره‌برداری از آسیب‌پذیری‌های Exchange مایکروسافت برای اکسپلویت مشتریان هستند.

۲۲ اسفند

یک آسیب‌پذیری روز صفرم دیگر در مرورگر کروم شناسایی و وصله شد!

گوگل با انتشار نسخه‌ی ۸۹/۰/۴۳۸۹/۹۰ مرورگر کروم برای سیستم‌های عامل ویندوز، مک و لینوکس، در مجموع ۵ آسیب‌پذیری را وصله کرد.

مهم‌ترین این آسیب‌پذیری‌ها، یک اشکال روز صفرم است که به صورت فعال مورد بهره‌برداری قرار می‌گیرد. این آسیب‌پذیری که با شناسه‌ی CVE-2021-21193 ردیابی می‌شود، از نوع use after free بوده و در موتور Blink مرورگر کروم شناسایی شده است.

۲۵ اسفند

با این ابزار و تنها با یک کلیک، آسیب‌پذیری در Exchange Server مایکروسافت را وصله کنید!

مایکروسافت به‌تازگی نرم‌افزاری را منتشر کرده که تمامی راه‌کارهای پیشگیری موردنیاز برای جلوگیری از حملات مبتنی بر آسیب‌پذیری‌های ProxyLogon Exchange Server را دارا ست.

این ابزار تنها با یک کلیک برای کاربران قابل استفاده است و Exchange On-premises Mitigation (EOMT) Tool نام دارد. این ابزار مبتنی بر پاورشل از بهره‌برداری آسیب‌پذیری CVE-2021-26855 جلوگیری می‌کند.

۲۶ اسفند

نسخه‌ی جدیدی از بدافزار و بات‌نت‌های Mirai در دنیای واقعی مشاهده شده است!

محققان امنیتی موج جدیدی از حملات سایبری را شناسایی کرده‌اند که دستگاه‌های متصل به اینترنت را با نسخه جدیدی از بدافزار Mirai هدف قرار داده‌اند.

با بهره‌برداری موفق از این آسیب‌پذیری‌های شل اسکریپت‌های مخرب در ادامه بدافزار Mirai را دانلود و نصب کرده و حمله‌ی brute-forcers را اجرا می‌کنند.

۲۶ اسفند

بات‌نت Zhtrap مبتنی بر Mirai، قربانیان جدید را از طریق سیستم هانی‌پات به تله می‌اندازد!

محققان یک بات‌نت مبتنی بر Mirai را با نام Zhtrap شناسایی کرده‌اند که از سیستم‌های هانی‌پات برای به دام انداختن قربانیان بیشتر استفاده می‌کند.

در حالی‌که از سیستم‌های هانی‌پات برای به دام انداختن مهاجمان و کشف شیوه‌های حملات آن‌ها استفاده می‌شود، بات‌نت Zhtrap از تکنیک مشابهی استفاده کرده و از یک ماژول اسکن آدرس IP برای شناسایی آدرس‌های IP اهداف خود بهره می‌برد. در ادامه نیز سیستم‌های شناسایی‌شده را هدف حمله قرار می‌دهد.