خبرنامه الکترونیکی ۷۶

مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

امنیت هوشمندانه در سازمان (بخش دوم)

شماره هفتاد و ششم، سال نهم، اردیبهشت ۱۴۰۵ | کاری از تیم تولید محتوای مرکز تخصصی آپای دانشگاه سمنان

https://cert.semnan.ac.ir info.cert@semnan.ac.ir ۰۲۳-۳۱۵۳۵۰۲۱ @semcert

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

اخبار امنیت سایبری

کشف آسیب پذیری در Axios

Axios یک کتابخانه بسیار پرکاربرد برای ارسال درخواست‌های HTTP در Node.js و مرورگر است و در بسیاری از برنامه‌های وب، APIها و سرویس‌های cloud-connected استفاده می‌شود. اخیراً یک آسیب‌پذیری مهم با شناسه CVE-۲۰۲۶-۴۰۱۷۵ در این کتابخانه منتشر شده که طبق advisory رسمی Axios/GitHub، می‌تواند یک Prototype Pollution در dependencyهای دیگر را به اجرای کد از راه دور (RCE) یا حتی تصرف کامل محیط ابری از طریق دور زدن AWS IMDSv۲ تبدیل کند. در توضیح رسمی آمده که ریشه مشکل به عدم پاک‌سازی مناسب headerها در کنار قابلیت‌های پیش‌فرض HTTP/SSRF در Axios برمی‌گردد. advisory رسمی شدت آن را Critical با CVSS ۹.۹ اعلام کرده است .

محصولات تحت تاثیر:

Axios (npm package)

نسخه‌های آسیب‌پذیر شامل شاخه x.۱ قبل از ۱.۱۵.۰ و شاخه x.۰ قبل از ۰.۳۱.۰ هستند.

این مشکل در نسخه‌های ۱.۱۵.۰ و ۰.۳۱.۰ برطرف شده است.

توصیه های امنیتی:

به‌روزرسانی فوری: به تمامی تیم‌های توسعه و سازمان‌ها توصیه می‌شود Axios را در اولویت اول به ۱.۱۵.۰ یا ۰.۳۱.۰ و ترجیحاً آخرین نسخه پایدار ارتقا دهند.

بررسی dependency chain: چون این آسیب‌پذیری در قالب یک gadget chain عمل می‌کند، صرفاً بررسی نسخه مستقیم Axios کافی نیست و باید وجود Prototype Pollution در dependency های جانبی نیز بررسی شود.

پایش دسترسی به metadata سرویس‌های ابری: در محیط‌های AWS و زیرساخت‌های cloud، درخواست‌های غیرعادی به metadata service و الگوهای مشکوک header manipulation باید بررسی شوند؛ چون advisory رسمی از سناریوی AWS IMDSv۲ bypass نام برده است.

کشف آسیب پذیری در Dgraph

آسیب‌پذیری CVE-۲۰۲۶-۴۱۴۹۲ با شدت ۹.۸ در Dgraph، یک پایگاه‌داده متن‌باز توزیع‌شده مبتنی بر GraphQL، باعث افشای خط فرمان پردازش از طریق endpoint بدون احراز هویت /debug/vars در مؤلفه Alpha می‌شود. در بسیاری از استقرارها، توکن مدیریتی از طریق گزینه راه‌اندازی "... = security "token - - تنظیم می‌شود؛ بنابراین افشای خط فرمان می‌تواند منجر به افشای توکن ادمین شود مهاجم می‌تواند این توکن را در هدر X-Dgraph-AuthToken بازاستفاده کند و به endpointهای مدیریتی Dgraph دسترسی غیرمجاز بگیرد. طبق GitHub Advisory، این مشکل گونه‌ای از آسیب‌پذیری قبلی مربوط به /debug/pprof/cmdline است، اما اصلاح قبلی کامل نبوده؛ زیرا فقط مسیر قبلی مسدود شده و http.DefaultServeMux همچنان handler مربوط به expvar و مسیر /debug/vars را ارائه می‌کند.

محصولات تحت تاثیر:

github.com/dgraph-io/dgraph/v۲۵ نسخه‌های قبل از ۲۵.۳.۳

برای شاخه‌های قدیمی‌تر، اطلاعات Advisory وضعیت متفاوتی نشان می‌دهد: github.com/dgraph-io/dgraph/v۲۴ تا ۲۴.۱.۸ و github.com/dgraph-io/dgraph تا ۱.۲.۸ به‌عنوان affected آمده‌اند، اما patched version برای آن‌ها مشخص نشده است

توصیه های امنیتی:

ارتقا به نسخه ۲۵.۳.۳ یا نسخه اصلاح‌شده متناظر با شاخه مورد استفاده.

محدود کردن دسترسی شبکه‌ای به پورت HTTP مربوط به Dgraph Alpha.

جلوگیری از دسترسی عمومی به endpointهای debug مانند /debug/vars.

چرخش/تغییر توکن‌های مدیریتی در صورتی که احتمال دسترسی غیرمجاز به endpointهای debug وجود داشته باشد.

بررسی لاگ‌ها برای درخواست‌های مشکوک به مسیرهای /debug/vars و endpointهای مدیریتی

APACHE®

Camel

کشف آسیب پذیری در Apache Camel

آسیب‌پذیری CVE-۲۰۲۶-۳۳۴۵۳ مربوط به مؤلفه camel-coap در Apache Camel است و ناشی از کنترل نامناسب روی attributeهای پویای ورودی است. در این آسیب‌پذیری، مؤلفه camel-coap پارامترهای query مربوط به درخواست‌های CoAP را بدون اعمال HeaderFilterStrategy مستقیماً به headerهای پیام Camel منتقل می‌کند. این موضوع امکان تزریق header های داخلی Camel را برای مهاجم فراهم می‌کند. در صورتی که route آسیب‌پذیر پیام‌های دریافتی از coap:// را به producerهای حساس به header مانند camel-file، camel-bean، camel-sql، camel-exec یا template component ها ارسال کند، مهاجم می‌تواند رفتار producer را تغییر دهد. در سناریوی header، camel-exec های تزریق‌شده می‌توانند executable و آرگومان های دستور را تغییر داده و منجر به اجرای دستور سیستم‌عامل با سطح دسترسی فرایند Apache Camel شوند

محصولات تحت‌تأثیر:

این آسیب‌پذیری مؤلفه org.apache.camel:camel-coap در Apache Camel را تحت تأثیر قرار می‌دهد.

نسخه‌های آسیب‌پذیر اعلام‌شده عبارت‌اند از:

- Apache Camel ۴.۱۴.۰ تا ۴.۱۴.۵
- Apache Camel ۴.۱۸.۰ قبل از ۴.۱۸.۱
- Apache Camel ۴.۱۹.۰

توصیه های امنیتی:

با توجه به شدت ۱۰.۰، امکان بهره‌برداری بدون احراز هویت و وجود PoC عمومی، سازمان‌هایی که از Apache Camel در سامانه های API Gateway، backend، یکپارچه‌سازی سرویس‌ها یا پردازش پیام استفاده می‌کنند باید این آسیب‌پذیری را در اولویت بررسی قرار دهند. این مورد به‌ویژه برای محیط‌هایی اهمیت دارد که مؤلفه camel-coap فعال است یا مسیرهای CoAP به producerهای حساس متصل شده‌اند.

این آسیب‌پذیری از نظر ماهیت، بیشتر در حوزه کتابخانه /API، Dependency، سرویس‌های سازمانی و Backend Integration قرار می‌گیرد و برای حوزه کاری وب‌اپلیکیشن و تست نفوذ وب نیز ارتباط متوسط رو به بالا دارد؛ زیرا می‌تواند در لایه سرویس‌های پشت‌صحنه و مسیرهای API/Integration منجر به RCE شود

کشف آسیب پذیری در MegaCMS

آسیب‌پذیری CVE-۲۰۲۶-۳۳۲۵ یک نقص از نوع SQL Injection در MegaCMS نسخه ۱۲.۰.۰ است. این آسیب‌پذیری در پارامتر id_territorio مربوط به endpoint زیر قرار دارد:

web_comunications/cms/get_provincias/

طبق اعلام INCIBE-CERT، این پارامتر در یک درخواست POST و پس از ارسال فرم ثبت‌نام استفاده می‌شود و به دلیل اعتبارسنجی و پاک‌سازی ناکافی ورودی، مهاجم بدون احراز هویت می‌تواند مقدار آن را دستکاری کند و کوئری‌های SQL دلخواه را اجرا کند. این نقص با شناسه CWE-۸۹ ثبت شده و امتیاز CVSS v۴.۰ برابر ۱۰.۰ دارد. بردار حمله آن شبکه‌ای است، پیچیدگی حمله پایین است، نیاز به دسترسی قبلی یا تعامل کاربر ندارد و اثر آن روی محرمانگی، یکپارچگی و دسترس پذیری سامانه بالا ارزیابی شده است.

محصولات تحت تاثیر:

MegaCMS نسخه ۱۲.۰.۰

INCIBE-CERT این آسیب‌پذیری را برای MegaCMS نسخه ۱۲.۰.۰ اعلام کرده است و در داده‌های OpenCVE نیز همین نسخه به‌عنوان affected ثبت شده است. نسخه‌های دیگر در منابع بررسی‌شده به‌صورت قطعی آسیب‌پذیر اعلام نشده‌اند

توصیه های امنیتی:

با توجه به اینکه این آسیب‌پذیری بدون نیاز به احراز هویت و از راه دور قابل سوءاستفاده است، سازمان‌هایی که از MegaCMS استفاده می‌کنند باید بررسی نسخه و اعمال به‌روزرسانی را در اولویت قرار دهند. این مورد برای سامانه‌های رزرو، فروش آنلاین، ticketing و سرویس‌هایی که اطلاعات کاربران را در پایگاه‌داده نگهداری می‌کنند اهمیت بیشتری دارد؛ زیرا SQL Injection می‌تواند منجر به افشای داده، تغییر داده یا اختلال در سرویس شود.

کشف آسیب‌پذیری در cPanel and WHM

آسیب‌پذیری با شناسه CVE-۲۰۲۶-۴۱۹۴۰ با شدت ۹.۸ (Critical) در نرم‌افزار cPanel & WHM شناسایی شده است. این آسیب‌پذیری از نوع Authentication Bypass بوده و در نتیجه ضعف در مدیریت نشست (Session Handling) و اعتبارسنجی ورودی در فرآیند احراز هویت سرویس cpsrvd ایجاد می‌شود. در این سناریو، مهاجم بدون نیاز به احراز هویت، با دستکاری کوکی نشست (به‌ویژه حذف بخش رمزنگاری‌شده آن) و ارسال درخواست حاوی هدر Authorization شامل کاراکترهای CRLF، ساختار فایل نشست را دچار اختلال می‌کند. این امر موجب می شود داده‌های نشست به‌جای یک مقدار یکپارچه، به چندین خط مجزا تفکیک شده و امکان درج مقادیر جعلی فراهم گردد. در ادامه، مهاجم با تزریق مقادیری نظیر hasroot=1، user=root و tfa_verified=1 در فایل نشست، و سپس تحریک فرآیند بازپارسی (re-parse) از طریق ارسال درخواست‌های خاص (مانند ایجاد خطای token_denied)، باعث می‌شود این مقادیر به‌عنوان بخشی از نشست معتبر تفسیر شوند. در نتیجه، سطح دسترسی نشست به سطح کاربر root ارتقاء می‌یابد. این آسیب‌پذیری بدون نیاز به احراز هویت و تنها از طریق دسترسی شبکه قابل بهره‌برداری بوده و به مهاجم امکان می‌دهد فرآیند ورود به سیستم را به‌طور کامل دور زده و به پنل مدیریتی با سطح دسترسی بالا دست یابد. بهره‌برداری موفق از این ضعف می‌تواند منجر به تصرف کامل سرور، دسترسی به اطلاعات حساس، تغییر تنظیمات و اجرای دستورات مدیریتی گردد و تهدیدی جدی برای محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات محسوب می‌شود.

محصولات تحت تاثیر:

تمامی نسخه‌های نرم‌افزار cPanel & WHM در بازه‌های زیر در برابر آسیب‌پذیری CVE-۲۰۲۶-۴۱۹۴۰ آسیب‌پذیر هستند:

۱۱.۱۱۰.۰.۰ - ۱۱.۱۱۰.۰.۹۶،۱۱.۱۱۸.۰.۰ - ۱۱.۱۱۸.۰.۶۲،۱۱.۱۲۶.۰.۰ - ۱۱.۱۲۶.۰.۵۳

۱۱.۱۳۲.۰.۰ - ۱۱.۱۳۲.۰.۲۸،۱۱.۱۳۴.۰.۰ - ۱۱.۱۳۴.۰.۱۹،۱۱.۱۳۶.۰.۰ - ۱۱.۱۳۶.۰.۴

توصیه های امنیتی:

دسترسی به پورت‌های مدیریتی (۲۰۸۳ / ۲۰۸۷) باید فقط از طریق IPهای مجاز (Whitelist) یا VPN سازمانی محدود شود. همچنین توصیه می شود دسترسی مستقیم از اینترنت عمومی به WHM به‌طور کامل مسدود گردد.

استفاده از Web Application Firewall برای شناسایی و مسدودسازی درخواست‌های مشکوک (به‌ویژه تغییرات غیرعادی در Cookie و Header) ضروری است.

اطمینان از اعمال وصله امنیتی با اجرای دستور زیر:

usr/local/cpanel/cpanel -V/

کشف آسیب پذیری در GeoVision

آسیب‌پذیری CVE-۲۰۲۶-۴۲۳۶۹ یک نقص بحرانی از نوع Stack Overflow در قابلیت WebCam Server نرم‌افزار GeoVision GV-VMS V۲۰ است. GV-VMS یک سامانه مدیریت ویدئو برای دریافت و مدیریت تصویر دوربین‌های نظارتی است و قابلیت WebCam Server امکان دسترسی راه‌دور به نمایش زنده و ویدئوهای ضبط‌شده از طریق مرورگر وب را فراهم می‌کند.

این آسیب‌پذیری در مکانیزم احراز هویت endpoint مربوط به `gvapi` رخ می‌دهد. در این بخش، رشته Base۶۴ رمزگشایی‌شده بدون کنترل مناسب اندازه در یک متغیر stack کپی می‌شود و در صورت ارسال درخواست HTTP دستکاری‌شده، مهاجم می‌تواند باعث سرریز بافر شود. طبق اطلاعات منتشرشده، نبود ASLR در WebCam Server بهره‌برداری را ساده‌تر کرده و موفقیت حمله می‌تواند به اجرای کد با سطح دسترسی SYSTEM روی سامانه میزبان منجر شود.

محصولات تحت تاثیر:

GeoVision GV-VMS V۲۰ نسخه ۲۰/۰/۲

این آسیب‌پذیری زمانی اهمیت بیشتری دارد که قابلیت WebCam Server فعال باشد و امکان دسترسی شبکه‌ای یا اینترنتی به رابط وب سامانه وجود داشته باشد. GV-VMS در محیط‌های نظارت تصویری و سازمانی استفاده می‌شود و WebCam Server برای دسترسی از راه دور از طریق مرورگر، موبایل و Remote ViewLog کاربرد دارد.

توصیه های امنیتی:

با توجه به شدت بحرانی آسیب‌پذیری و امکان اجرای کد از راه دور، سازمان‌هایی که از GeoVision GV-VMS V۲۰ استفاده می‌کنند باید وضعیت نسخه نرم‌افزار و فعال بودن WebCam Server را بررسی کنند.

در صورت استفاده از نسخه آسیب‌پذیر، توصیه می‌شود نرم‌افزار از صفحه رسمی دانلود GeoVision به آخرین نسخه موجود به‌روزرسانی شود، دسترسی عمومی به WebCam Server محدود گردد و تا زمان اعمال اصلاحیه، دسترسی به این سرویس فقط از طریق شبکه داخلی یا VPN مجاز باشد. همچنین بررسی لاگ‌های HTTP و درخواست‌های مشکوک به endpointهای مربوط به `gvapi` پیشنهاد می شود.

کشف آسیب‌پذیری اجرای کد از راه دور در Cisco Secure FMC

یک آسیب‌پذیری بحرانی با شناسه CVE-۲۰۲۶-۲۰۱۳۱ در محصول Cisco Secure Firewall Management Center (FMC) شناسایی و منتشر شده است. این آسیب‌پذیری از نوع اجرای کد از راه دور (Remote Code Execution - RCE) بوده و می‌تواند به مهاجم غیرمجاز اجازه دهد بدون نیاز به احراز هویت، کد دلخواه خود را بر روی سامانه آسیب‌پذیر اجرا کند.

بر اساس اطلاعیه امنیتی منتشرشده توسط شرکت سیسکو، ریشه این آسیب‌پذیری در فرآیند ناامن deserialization داده‌های جاوا در رابط مدیریتی تحت وب FMC قرار دارد. مهاجم می‌تواند با ارسال یک شیء Java Serialized دست‌کاری‌شده به رابط مدیریتی وب، این نقص را مورد سوءاستفاده قرار داده و در صورت موفقیت، کد دلخواه خود را با سطح دسترسی root روی دستگاه اجرا کند.

با توجه به سطح دسترسی به‌دست‌آمده در صورت بهره‌برداری موفق، این آسیب‌پذیری می‌تواند پیامدهای امنیتی جدی برای سازمان‌ها به همراه داشته باشد که از جمله آن‌ها می‌توان به موارد زیر اشاره کرد:

اجرای کد مخرب بر روی سامانه مدیریت فایروال

دسترسی کامل مهاجم به سطح دسترسی(root) در دستگاه

امکان تغییر یا دستکاری تنظیمات امنیتی فایروال

ایجاد دسترسی پایدار در زیرساخت شبکه و گسترش حمله در محیط سازمانی

امتیاز شدت این آسیب‌پذیری بر اساس استاندارد CVSS در سطح بحرانی (Critical) و با امتیاز ۱۰.۰ ارزیابی شده است. در صورتی که رابط مدیریتی FMC به اینترنت عمومی در دسترس باشد، احتمال سوءاستفاده از این آسیب‌پذیری به‌طور قابل توجهی افزایش می‌یابد.

شرکت سیسکو برای رفع این مشکل به‌روزرسانی‌های امنیتی منتشر کرده و اعلام نموده است که هیچ راهکار موقتی (Workaround) برای رفع کامل این آسیب‌پذیری وجود ندارد.

توصیه های امنیتی:

به‌روزرسانی فوری Cisco Secure Firewall Management Center به نسخه‌های اصلاح‌شده منتشرشده توسط سیسکو

محدودسازی دسترسی به رابط مدیریتی FMC و جلوگیری از دسترسی مستقیم آن از اینترنت عمومی

اعمال سیاست‌های کنترلی شبکه و محدودسازی دسترسی مدیریتی صرفاً به IPهای مورد اعتماد

با توجه به ماهیت بحرانی این آسیب‌پذیری و امکان اجرای کد با سطح دسترسی ریشه، عدم اعمال اصلاحیه‌های امنیتی می‌تواند زیرساخت‌های شبکه سازمان را در معرض خطر جدی قرار دهد؛ بنابراین انجام اقدامات اصلاحی و اعمال به‌روزرسانی‌های امنیتی در اسرع وقت ضروری است.

مرکز آپا دانشگاه سمنان

امنیت هوشمندانه در سازمان

مدیریت رمزهای عبور و احراز هویت امن در محیط‌های کاری

در بخش اول این مجموعه، درباره نقش کارمندان در امنیت سازمان و تهدیدات روزمره مانند فیشینگ، مهندسی اجتماعی و استفاده از ابزارهای ناشناس صحبت کردیم.

اما یکی از مهم‌ترین و ابتدایی‌ترین نقاط ضعف در بیشتر سازمان‌ها چیزی بسیار ساده است: رمزهای عبور ضعیف یا تکراری.

بخش دوم به کمک شما می‌آید تا بدون نیاز به دانش تخصصی، خط دفاع اول سازمان را محکم‌تر کنید.

۱. چرا رمز عبور مهم‌ترین نقطه حمله است؟

تحقیقات جهانی نشان می‌دهد که:

- حدود ٪۸۱ از نفوذهای موفق، به واسطه رمز عبور ضعیف یا لو رفته رخ می‌دهند.
- بیش از ٪۵۰ کارمندان از یک رمز مشترک برای چند سامانه استفاده می‌کنند.
- بسیاری از رمزها از روی اطلاعات شخصی قابل حدس هستند (تاریخ تولد، شماره تلفن، نام فرزندو...).

برای مهاجم، نیازی به شکستن رمزهای پیچیده نیست؛

او همان رمزی را امتحان می‌کند که شما از روی راحتی انتخاب کرده‌اید.

۲. ویژگی‌های یک رمز عبور امن

یک رمز عبور امن لزوماً سخت نیست؛ هوشمندانه است.

ویژگی‌های اصلی:

- حداقل ۱۰ تا ۱۲ کاراکتر
- ترکیب حروف کوچک، بزرگ، اعداد و علامت‌ها
- غیرقابل حدس از روی اطلاعات شخصی
- عدم استفاده در چند سامانه مختلف

رمزهای زیر ناامن هستند:

- ۱۲۳۴۵۶
- @Password
- شماره تلفن
- تاریخ تولد
- نام فرزند یا همسر

نمونه رمزهای امن:

- S۳۳na!Cloud*۲۰۲۶
- L!ght_Stairs۹۲۷
- Sky#Door!۴۴۱۲

(نیازی نیست پیچیده و غیرقابل حفظ باشد؛ فقط هوشمند و ترکیبی باشد.)

امنیت هوشمندانه در سازمان (بخش دوم)

۳. اشتباهات رایج در استفاده از رمز عبور

در بسیاری از سازمان‌ها مشکلات امنیتی ناخواسته از همین اشتباهات ساده شروع می‌شود:

- چسباندن رمز روی مانیتور یا گذاشتن داخل کشوی میز
- ذخیره رمز در فایل Word یا Excel بدون رمزگذاری
- ارسال رمز عبور از طریق پیام‌رسان‌ها
- استفاده از رمز مشابه برای حساب شخصی و سازمانی
- عدم تغییر رمز پس از دریافت پیام مشکوک
- استفاده از مرورگر به‌عنوان حافظه رمز بدون بررسی امنیتی

این‌ها مواردی هستند که مهاجم عاشق‌شان است.

۴. بهترین روش ساخت و مدیریت رمزها: روش «عبارت رمز»

رمز پیچیده لزوماً بهتر نیست؛ رمز قابل حفظ که طولانی و ترکیبی باشد، به‌مراتب امن‌تر است.

بهترین روش برای کاربران سازمانی استفاده از عبارت‌های رمز (Passphrase) است.

مثال:

«S۳mnan!Univ!Spring۱۴۰۳»

یا:

«BlueCar!GoesFast@۸۹»

مزیت‌ها:

- طولانی است ⟵ سخت‌تر شکسته می‌شود
- حفظ آن آسان است
- قابل سفارشی‌سازی برای هر سامانه
- نیاز به نوشتن ندارد

امنیت هوشمندانه در سازمان (بخش دوم)

۵. احراز هویت چندمرحله‌ای (MFA): سپر دفاعی دوم

حتی بهترین رمز هم ممکن است فاش شود. برای همین بسیاری از سازمان‌ها از روش احراز هویت چندمرحله‌ای استفاده می‌کنند؛ یعنی علاوه بر رمز، یک کد یک‌بارمصرف یا تأیید هویت اضافه لازم است.

رایج‌ترین روش‌ها:

- ارسال کد پیامکی
- استفاده از اپلیکیشن‌های تولید کد (Authenticator)
- تأیید دستگاه‌های مورد اعتماد
- کلیدهای امنیتی سخت‌افزاری

کارمندانی که MFA فعال دارند، بیش از ٪۹۹ از حملات نفوذ با رمز عبور در امان هستند.

۶. ۶ توصیه IMPORTANT برای کارمندان سازمان

برای استفاده امن از رمزها، اجرای این ۶ اصل کافی است:

۱. رمزهای تکراری برای سامانه‌های مختلف نگذارید.

۲. رمزهای خود را با هیچ‌کس–even پشتیبانی سازمان–به اشتراک نگذارید.

۳. در پیام‌ها یا تماس‌های ناشناس، رمز را اعلام نکنید.

۴. از ذخیره خودکار رمز در مرورگرهای قدیمی خودداری کنید.

۵. اگر حتی کمی شک کردید (ایمیل عجیب، پیام عجیب، رفتار غیرمعمول سامانه)، رمز را تغییر دهید.

۶. برای سامانه‌های مهم، MFA را فعال کنید.

۷. به‌روزرسانی رمز عبور: کی لازم است؟

در این موارد رمز باید فوراً تغییر کند:

- پس از باز کردن یک ایمیل یا لینک مشکوک
- پس از دریافت پیام خطاها یا ورودهای ناشناس
- پس از استفاده از سیستم در مکان‌های عمومی
- بعد از گم‌شدن یا تعمیر دستگاه کاری
- هنگام ترک یا تغییر پست سازمانی

بهتر است رمزهای اصلی حداقل هر ۶ ماه به‌روزرسانی شوند.

امنیت هوشمندانه در سازمان (بخش دوم)

۸. نکاتی درباره ذخیره امن رمزها

اگر تعداد رمزها زیاد است، استفاده از مدیر رمز (Password Manager) بهترین گزینه است.

مزایا:

- فقط یک رمز اصلی حفظ می‌کنید
- رمزهای قوی و تصادفی تولید می‌کند
- رمزها را به‌صورت رمزگذاری‌شده ذخیره می‌کند
- خطای انسانی را کاهش می‌دهد

نمونه‌های رایج: KeePass، 1Password، Bitwarden

(در نسخه سازمانی استفاده شود.)

۹. جمع‌بندی: رمزهای عبور، کوچک اما حیاتی

در این شماره آموختیم:

- رمز عبور، اولین هدف مهاجمان است.
- ساخت رمزهای طولانی و مبتنی بر «عبارت رمز» بهترین روش برای کاربران سازمانی است.
- اشتباهات کوچک مثل نوشتن رمز یا ارسال آن در پیام‌رسان می‌تواند به حادثه بزرگ تبدیل شود.
- احراز هویت چندمرحله‌ای یکی از بزرگ‌ترین سپرهای امنیتی برای کارکنان است.

در بخش سوم این مجموعه، به سراغ موضوع جذاب و بسیار کاربردی زیر می‌رویم:

چگونه پیام‌ها، ایمیل‌ها و لینک‌های جعلی را سریع تشخیص دهیم؟

(با مثال، نکته‌های واقعی و چک‌لیست مخصوص کارمندان)