Borna Network Managers
مدیران شبکه برنا

خبرنامه برنا

اخبار حوزه امنیت و شبکه (خرداد ۱۴۰۴)

خبرنامه تخصصی «مدیران شبکه برنا»؛ نگاهی حرفه‌ای به دنیای امنیت شبکه هر ماه با ما همراه باشید تا در جریان جدیدترین تهدیدات سایبری، تحلیل رویدادها، به‌روزرسانی محصولات و راهکارهای نوین امنیت اطلاعات قرار بگیرید.

ویژه مدیران و کارشناسان شبکه و امنیت
(رایگان، تخصصی، به‌روز)

www.bornanetwork.co
info@bornanetwork.co
۰۲۱-۷۴۰۲۸

وقتی نفوذ هم از قلب شبکه می آید، هم از اعماق سخت افزار

قصد داریم با بررسی حملات اخیر رخ داده در کشور را با تکنیک اجرای آن و تحلیل تیم فنی مجموعه برنا به نحوه عملکرد آن در سیستم‌ها بپردازیم.

در سال‌های اخیر، زیرساخت‌های حیاتی ایران صحنه حملاتی بی‌سابقه در تاریخ سایبری جهان بودند؛ که هر یک سبک و ویرانی متفاوتی را به نمایش گذاشتند. در یک سو، Stuxnet بود: بدافزاری مخفی و پیچیده که به عنوان نخستین سلاح سایبری جهان شناخته شد. Stuxnet با نفوذ هدفمند به سیستم های صنعتی و «دستیابی خاموش» سانتریفیوژهای نطنز، نشان داد آسیب‌های سایبری فقط محدود به دیتا و اطلاعات نیست، بلکه می‌تواند اثرات فیزیکی و جبران‌ناپذیری هم داشته باشد. این حمله، چشم انداز جهانی امنیت صنعتی را برای همیشه تغییر داد و صنعت را وارد دوران جدیدی از تهدیدات کرد.

در سوی دیگر، حملات اخیر سایبری مثل حملات گروه گنجشک درنده‌خوار قرار دارند که با سوءاستفاده از ماژول مدیریتی iLO سرورهای HPE، فصل تازه‌ای از مشکلات امنیتی را باز کردند. مهاجمان از طریق رمز عبور ضعیف یا آسیب‌پذیری‌های آپدیت‌نشده‌ی iLO، موفق شدند کنترل کامل فیزیکی و نرم‌افزاری سرورهای حیاتی را به دست گیرند و حتی با حذف و نابودی داده‌ها و سیستم‌عامل، در سطحی «غیرقابل جبران» به شبکه‌های صنعتی آسیب بزنند.

نقطه اشتراک این دو تهدید چیست؟

جنگ سایبری امروز، فقط جنگ نرم‌افزار و ویروس و Data نیست؛ بلکه تهدیدی ترکیبی است که هم نرم‌افزار، هم سخت‌افزار و حتی اپراتور انسانی را هدف می‌گیرد. غفلت از هر گوشه‌ای - چه مهندسی فرآیند باشد، چه دسترسی مدیریتی مثل iLO - می‌تواند نتایج فاجعه‌آمیزی به همراه داشته باشد.

نتیجه؟

حملات Stuxnet و iLO دو روی یک سکه‌اند:

- یکی با خرابکاری پنهان و مهندسی‌شده
- دیگری با تخریب مستقیم و تسخیر مدیریتی

هشدار بزرگ برای مدیران IT این است که امنیت سایبری فقط دیوارآتش و آنتی‌ویروس نیست؛ بلکه توجه جدی به کوچک‌ترین back-door و نقطه ضعف مدیریتی، حیاتی است.

آسیب‌پذیری بحرانی در پروتکل ریموت دسکتاپ

طبق گزارش مرکز ملی آسیب‌پذیری‌ها (NVD) و شناسایی ضعف امنیتی با کد CVE-2025-24035 و CVE-2025-24045، یک آسیب‌پذیری بحرانی در پروتکل ریموت دسکتاپ (RDP) ویندوز به ثبت رسیده است. این آسیب‌پذیری به مهاجمان اجازه می‌دهد با سوءاستفاده از قابلیت‌های RDP، کدهای مخرب را اجرا کرده و به سیستم‌های هدف دسترسی پیدا کنند. چنین ضعف امنیتی می‌تواند منجر به نفوذ جدی به اطلاعات حساس و اختلال در عملکرد سازمان‌ها شود.

سطح خطر:

این آسیب‌پذیری به‌عنوان بحرانی (Critical) طبقه بندی شده و به‌روزرسانی سریع و اقدامات پیشگیرانه برای جلوگیری از سوءاستفاده الزامی است.

اقدامات ضروری:

به‌روزرسانی ویندوز: از نصب آخرین Patchهای امنیتی مایکروسافت اطمینان حاصل کنید.

غیرفعال‌سازی دسترسی غیرضروری به RDP: پورت های مرتبط با پروتکل 3389 فقط برای منابع معتبر باز باشند.

احراز هویت چندمرحله‌ای را فعال کنید: برای محافظت بیشتر.

استفاده از ابزارهای مانیتورینگ پیشرفته جهت شناسایی سریع حرکات مشکوک در شبکه.

بهره‌مندی از فایروال‌ها و نرم‌افزارهای ضدنفوذ به‌روزرسانی‌شده.

هشدار مهم امنیتی درباره بدافزار JaskaGO

بر اساس گزارش‌های امنیتی منتشر شده از سوی مرکز مدیریت راهبردی افتا و AT&T Alien Labs، بدافزار جدیدی با نام JaskaGO که با زبان برنامه نویسی Go توسعه یافته است، به عنوان یکی از تهدیدهای پیشرفته و چندسکویی، سیستم‌عامل‌های ویندوز و macOS را هدف قرار داده است.

این بدافزار از سال 2023 فعال بوده و با روش‌های مختلف از جمله جعل فایل‌های نصب نرم‌افزارهای معتبر مانند CapCut و AnyConnect، کاربران را آلوده می‌کند. پس از نصب، بدافزار بررسی می‌کند آیا برنامه در محیط مجازی اجرا می‌شود یا خیر و در صورت صحت، رفتار خود را تغییر می‌دهد تا شناسایی نشود.

قابلیت‌های JaskaGO شامل:

برداشت اطلاعات حساس از سیستم قربانی

برقراری ارتباط با سرور فرماندهی جهت دریافت دستورات مخرب، اجرای دستورات و دانلود بدافزارهای دیگر

تغییر محتوای کلیپ‌بورد برای سرقت ارزهای دیجیتال

جمع‌آوری فایل‌ها و داده‌های ذخیره‌شده در مرورگر

ایجاد پایداری بالا در macOS با غیرفعال‌سازی "Gate-keeper" و ساخت سرویس اختصاصی برای اجرا در هر بار راه‌اندازی

تحقیقات نشان می‌دهد انتشار این بدافزار اغلب با روش‌های فیشینگ یا تبلیغات مخرب انجام می‌شود، اما همچنان ابعاد کامل این کمپین روشن نشده است.

توصیه‌های امنیتی:

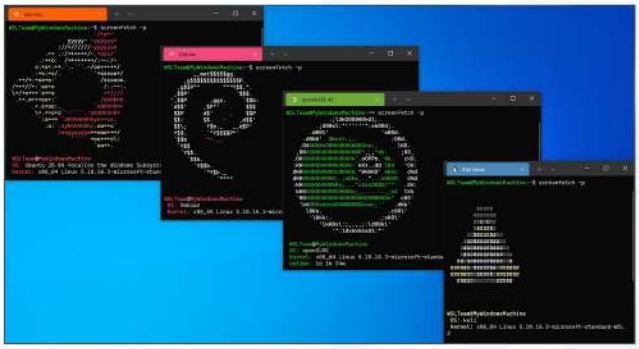
به‌روز نگه داشتن سیستم‌عامل و نرم‌افزارها

استفاده از راهکارهای امنیتی و آنتی‌ویروس معتبر

پرهیز از دانلود و اجرای برنامه‌های ناشناس و نامطمئن

افزایش آگاهی و آموزش پرسنل و کاربران در خصوص حملات سایبری

ویندوز ساب سیستم برای لینوکس (WSL) اکنون متن باز است



مایکروسافت به تازگی اعلام کرده است که پروژه ویندوز ساب‌سیستم برای لینوکس (WSL) به صورت متن‌باز در اختیار جامعه توسعه‌دهندگان قرار گرفته است. این تصمیم، گام مهمی در جهت افزایش شفافیت، جلب مشارکت بیشتر و هم‌افزایی با برنامه نویسان و علاقه‌مندان حوزه نرم‌افزارهای متن‌باز به شمار می‌آید.

با متن‌باز شدن WSL، تمامی علاقه‌مندان می‌توانند به کد منبع این پروژه دسترسی داشته باشند، پیشنهادات و ابتکارات خود را مطرح کنند و در بهبود قابلیت‌ها و عملکرد آن سهیم باشند. همچنین این امکان فراهم شده تا با همکاری جامعه جهانی، فرآیند کشف و رفع اشکالات و افزودن قابلیت‌های جدید به WSL سرعت بیشتری پیدا کند.

آسیب‌پذیری حیاتی در Cisco Prime Collaboration Deployment

CVE-2024-20319

بر اساس گزارش رسمی مرکز ملی آسیب‌پذیری آمریکا (NVD)، یک آسیب‌پذیری بحرانی با شناسه CVE-2024-20319 در زیرساخت نرم‌افزار Cisco Prime Collaboration Deployment کشف شده است.

این آسیب‌پذیری به مهاجم غیرمجاز اجازه می‌دهد دستورات دلخواه را با دسترسی سطح root از طریق API به‌طور مستقیم بر روی سرور آسیب‌پذیر اجرا نماید.

شرح فنی:

نوع آسیب‌پذیری: اجرای فرمان از راه دور (Remote Code Execution)

بردار حمله: از طریق REST API آسیب‌پذیر، بدون نیاز به احراز هویت

امتیاز شدت (CVSS): 9.8 (بحرانی)

نسخه‌های آسیب‌پذیر: تمامی نسخه‌های اعلام‌شده توسط Cisco در اطلاعیه رسمی

ریسک: تصرف کامل سیستم و تهدید جدی برای یکپارچگی و محرمانگی داده‌ها

اقدامات لازم:

هرچه سریع‌تر به‌روزرسانی رسمی Cisco را نصب نمایید.

دسترسی عمومی به REST API را تا زمان رفع کامل آسیب‌پذیری محدود یا مسدود کنید.

وضعیت به‌روزرسانی سامانه‌ها را به‌طور مستمر پایش نمایید.

کشف آسیب‌پذیری بحرانی در پردازنده‌های اینتل

محققـان دانشـگاه ETH زوریـخ یـک کلاس جدیـد از آسـیب‌پذیری‌ها بـه نـام BPRC (Branch Predictor Race Conditions) را در تمـام پردازنده‌هـای اینتـل از سـال ۲۰۱۸ کشـف کرده‌انـد. ایـن نقص‌هـا، بـا شناسـه هـای CVE-2024-45332، CVE-2024-28956 و CVE-2025-24495، بـه مهاجمـان اجـازه می‌دهنـد داده هـای حسـاس ماننـد رمزهـای عبـور، کلیدهـای رمزنـگاری و اطلاعـات خصوصـی را از حافظـه پردازنـده اسـتخراج کننـد. ایـن تهدیـد بـرای محیط‌هـای ابـری چندکاربـره و دستگاه‌های شخصی خطرناک است.

جزئیات آسیب‌پذیری BPRC چیست؟

شناسـه‌ها: CVE-2024-45332، CVE-2024-28956، CVE-2025-24495

نـوع تهدیـد: نشـت داده از طریـق شـرایط رقابتـی پیـش بینی شاخه (Branch Predictor Race Conditions)

شـدت خطـر: بـالا (امتیـاز CVSS: اعلام‌نشـده، امـا بهـره برداری محتمل)

تأثیـر: مهاجمـان می‌تواننـد بـا بهره‌بـرداری از فنـاوری اجـرای گمانـه‌زن (speculative execution)، موانـع امنیتـی را دور زده و محتـوای حافظـه کـش و RAM کاربـران دیگـر را بـا سـرعت بیـش از ۵۰۰۰ بایـت بـر ثانیـه بخوانند.

www.bornanetwork.co info@bornanetwork.co ۰۲۱-۷۴۰۲۸

ابزار Wazuh Vulnerability Explorer

بحرانی در پروتکل ریموت دسکتاپ

CTI Wazuh یک پایگاه داده جامع از آسیب‌پذیری‌ها را در اختیار شما قرار می‌دهد تا به سرعت ریسک های احتمالی را شناسایی و مدیریت کنید.

دسترسی به جدیدترین CVEها و اجرای آن در سیستم عامل های مختلف براسا منابعی همچون NVD

*مشاهده درجه‌بندی شدت (severity)

راهکارهای کاهش ریسک و مقابله با حملات سایبری با توجه به متدهای Mitre ATT&CK

این ابزار از پلتفرم‌های Linux، MacOS و Windows پشتیبانی می‌کند و به شما کمک می‌کند امنیت شبکه و داده‌های سازمان خود را ارتقا دهید.

تازه‌ترین آسیب‌پذیری‌های critical و high severity هر هفته به‌روزرسانی می‌شوند.

بانک اطلاعاتی بیش از ۲۹۶,۶۰۰ آسیب‌پذیری (Signa-ture)