مرکز مدیریت آمار و فناوری اطلاعات
وزارت بهداشت، درمان و آموزش پزشکی

بسمه تعالی

شماره : د/۱۱۰/۵۴۰
تاریخ : ۱۴۰۲/۰۴/۰۳
پیوست : دارد

مهار تورم و رشد تولید
((مقام معظم رهبری))

مدیران محترم آمار و فناوری اطلاعات دانشگاه ها/دانشکده های علوم پزشکی و خدمات بهداشتی درمانی سراسر کشور

موضوع : توصیه نامه استفاده از محصولات نرم افزاری متن باز – Open Source

با سلام

احتراما، با عنایت به آسیب پذیری های اعلام شده برای برخی از محصولات نرم افزاری متن باز (Open Source) و استفاده برخی از دانشگاه های علوم پزشکی و واحدهای ستادی وزارت متبوع از این نرم افزارها، به پیوست فایل توصیه نامه استفاده از محصولات متن باز به حضور ارسال می گردد. خواهشمند است دستور فرمایید ضمن بررسی موارد ذکر شده، نسبت به انجام الزامات امنیتی پیشگیرانه اقدام فرمایند.

دکتر سید رضا مظهری
رییس مرکز مدیریت آمار و فناوری اطلاعات

شهرک قدس، خیابان سیمای ایران، بین فلامک و زرافشان، وزارت بهداشت، درمان و اموزش پزشکی،
بلوک A، طبقه پنجم، تلفن: ۲-۸۱۴۵۳۶۰۱ نمابر: ۸۱۴۵۶۵۰۳
نشانی اینترنتی: it.behdasht.gov.ir نشانی پست الکترونیکی: it@behdasht.gov.ir

این مستند به منظور ارائه توصیه های فنی و امنیتی در خصوص استفاده از محصولات نرم افزاری متن باز (Open Source) تهیه و تدوین گردیده است.

مقدمه :

نرم افزار اوپن سورس نرم‌افزاری با کد منبع (Source Code) باز است که هرکسی می تواند آن را بازرسی، اصلاح و تقویت نماید. نرم افزار منبع باز (OSS) نرم‌افزاری است که با کد منبع خود توزیع می‌شود و با استفاده از حقوق اصلی خود آن را برای استفاده، اصلاح و توزیع در دسترس قرار می‌دهد. توسعه دهندگان که به کد منبع دسترسی دارند می‌توانند با افزودن، تغییر یا اصلاح قسمت‌هایی از برنامه، آن را متناسب با نیاز خود تغییر دهند. ریسک نرم افزار های Open Source یا متن باز همیشه بالاست و استفاده از آنها ممکن است با چالش‌های متعددی همراه باشد. به همین دلیل استفاده از نرم افزار های متن باز می تواند خطراتی را برای استفاده کنندگان به همراه داشته باشد. این ریسک‌ها و خطرات، مشکلات کارکردی و امنیت سایبری را هم شامل می شوند.

مزایا و معایب نرم افزار منبع باز :

مزایا

- نرم افزارهای منبع باز در دسترس و انعطاف‌پذیر هستند. توسعه‌دهندگان می‌توانند نحوه کار کد را بررسی کرده و آزادانه در جنبه‌های ناکارآمد یا مشکل‌ساز برنامه تغییراتی ایجاد نمایند تا نیازهای منحصر به فرد آن‌ها را بهتر تطبیق دهند.
- کد منبع نرم افزارهای متن باز به صورت عمومی توزیع می‌شود، بنابراین کاربران می‌توانند برای پروژه‌های طولانی مدت خود به طور مداوم کد منبع را اصلاح و بهبود بخشند.
- مفهوم Zero Trust در بررسی کد سامانه های متن باز قابل اجرا است. با توجه با باز بودن منبع، امکان ارزیابی وجود آسیب پذیری،کدهای ناخواسته و یا مضر برای متخصصین، مشارکت کنندگان (Contributor) و یا مصرف کننده فراهم است.

- در صورت انتخاب با معیار های صحیح معمولا جامعه توسعه دهندگان خدمات و رفع اشکالات سریعی برای برنامه ارائه می کنند.

معایب

- نرم‌افزار متن باز می‌تواند مسئولیت‌هایی را ایجاد کند. برخلاف نرم‌افزارهای تجاری، که به طور کامل توسط فروشنده کنترل می‌شود، نرم افزارهای متن باز به ندرت شامل هرگونه ضمانت، مسئولیت یا محافظت از خسارت در برابر تخلف می‌باشند. این امر مسئولیت حفظ انطباق با تعهدات قانونی را به عهده مصرف کننده این نرم افزارها می‌گذارد.
- نرم افزار متن باز می‌تواند هزینه‌های غیرمنتظره ای را در آموزش کاربران، وارد کردن داده‌ها و تنظیمات نرم افزاری و بروز رسانی مورد نیاز تحمیل نماید.
- پشتیبانی فنی از نرم افزار های متن باز مشکل بوده و نیاز به تخصص بالا دارد. استفاده از این نرم افزار ها در محیط های عملیاتی و وابسته شدن عملیات سازمانی به این نرم افزار ها **بدون تخصص کافی**، مخاطراتی چون اختلال طولانی خدمت رسانی بر اثر مشکلات پیش بینی نشده و تحمیل هزینه های سنگین سازمانی را به همراه دارد.
- با توجه به دسترسی عمومی منبع برنامه، احتمال و امکان سوء استفاده از آن نیز به همین نسبت بالاتر خواهد رفت. این مورد مخصوصا در اپلیکیشن هایی که با اطلاعات مهم کاربران سر و کار دارند بیشتر مشاهده می شود. آسیب‌پذیری‌ها و نقاط ضعف در نرم‌افزارهای اپن سورس به اطلاع عموم رسانده می شود. در واقع این کار توسط خود مشارکت‌کنندگان و همچنین توسط سازمان‌هایی مثل پروژه امنیت برنامه‌های وب باز (OWASP) انجام می شود.

تدابیر امنیتی مقابله با مخاطرات نرم افزارهای متن باز :

- قرار دادن سامانه های مبتنی بر نرم افزارهای متن باز پشت Web Application Firewall یا WAF
- تبیین و پذیرش مسئولیت مرتبط با استفاده از نرم افزار توسط بهره بردار
- اخذ تاییدیه کمیته امنیت دستگاه
- غیرفعال نمودن دسترسی سرور سامانه به شبکه ی اینترنت و حدالامکان ایزوله نمودن کامل سرور در لایه شبکه
- ردیابی مستمر هشدارها و راهنمایی های امنیتی و CVE های مرتبط با محصول متن باز مورد استفاده و برطرف نمودن سریع آسیب پذیری های منتظر شده
- پیگیری مداوم و مستمر بروزرسانی های ارائه شده برای نرم افزار مربوطه و اعمال بروزرسانی ها جهت بهبود عملکرد سامانه و برطرف نمودن ایرادات احتمالی

- بررسی مستمر Log های مربوط به سامانه و ارسال Log ها به مرکز عملیات امنیت دستگاه جهت بررسی و ارزیابی های تکمیلی
- استفاده دوره ای از نرم افزاری های اسکن خودکار آسیب پذیری (Vulnerability Scanner) جهت شناسایی نقاط ضعف و آسیب پذیری های سامانه و برطرف نمودن آنها
- استفاده از نرم افزار های بومی فاقد گواهی افتا و گواهی اصالت نرم افزاری، نیز مانند نرم افزار های متن باز دارای ریسک بالای استفاده می باشد.
- تصمیم گیری و مسئولیت استفاده از نرم افزار های اشاره شده به عهده کمیته امنیت دستگاه می باشد.