

به نام خدا

پرو فایل حفاظتی برنامه های کاربردی تحت شبکه

اردیبهشت ماه ۹۶

نسخه ۱،۱

فهرست

۱.....	به نام خدا
۵.....	۱ مقدمه
۵.....	۲ اصطلاحات
۶.....	۳ شرح محصول
۸.....	۳,۱ مؤلفه های محیط عملیاتی
۱۱.....	۳,۲ انواع کاربران
۱۱.....	3.3 ویژگی های امنیتی محصول
۱۳.....	۴ مسائل امنیتی
۱۳.....	۴,۱ تهدیدات
۱۵.....	۴,۲ خطمشی امنیتی
۱۶.....	۴,۳ فرضیات
۱۷.....	۵ اهداف امنیتی
۱۷.....	۵,۱ اهداف امنیتی برای محصول
۲۰.....	۵,۲ اهداف امنیتی برای محیط عملیاتی
۲۱.....	۶ الزامات کارکرد امنیتی
۲۶.....	6.1 کلاس ممیزی امنیت
۳۸.....	۶,۲ کلاس پشتیبانی از رمزنگاری

۳۸.....	کلاس شناسایی و احراز هویت	۶,۳
۴۷.....	کلاس حفاظت از داده های کاربری	6.4
۵۷.....	کلاس مدیریت امنیت	6.5
۶۳.....	کلاس حفاظت از توابع امنیتی محصول	۶,۶
۶۸.....	کلاس دسترسی به محصول	۶,۷
۷۲.....	کلاس تخصیص منابع	۶,۸
۷۳.....	کلاس کانال ها/مسیرهای مورد اعتماد	۶,۹
۷۴.....	الزامات تضمین امنیت	۷
۷۵.....	کلاس توسعه	7.1
۷۸.....	کلاس راهنمای کاربر	7.2
۷۹.....	راهنمای کاربردی	۷,۲,۱
۸۱.....	راهنمای آماده سازی	۷,۲,۲
۸۳.....	کلاس آزمون	7.3
۸۴.....	آزمون مستقل	7.3.1
۸۵.....	کلاس آسیب پذیری	7.4
۸۵.....	تحلیل آسیب پذیری	۷,۴,۱
۸۷.....	کلاس پشتیبانی از چرخه حیات	7.5
۸۷.....	قابلیت های پیکربندی	7.5.1

۷,۵,۲	حوزه پیکربندی	۸۸
۸	پیوست یک: الزامات کلاس پشتیبانی از رمزنگاری مبتنی بر انتخاب	۸۹
۹	پیوست دو: الزامات پروتکل TLS مبتنی بر انتخاب	۹۲

۱ مقدمه

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده نمودن الزامات ارائه شده اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را بر اساس سند نظام ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 در راستای این هدف تهیه نموده است. این پرو فایل حفاظتی، به بیان الزامات برنامه کاربردی تحت شبکه می پردازد.

۲ اصطلاحات

مستند: به هر سندی که حاوی اطلاعات برای اجرا و پشتیبانی عملیات ها و فعالیت های سازمانی مورد استفاده قرار می گیرند، مستند گفته می شود.

رکورد: مستندی که اطلاعات فعالیت ها، رویدادها و نتایج حاصله را نگهداری می کند. به عبارت دیگر یک رکورد مستندی است که مدرک انجام یک فعالیتی مشخص است. یک رکورد می تواند شامل دو یا چند مستند باشد.

رکورد ممیزی: رکوردي که حاوی اطلاعات رویدادهایی است که برای ممیزی برنامه کاربردی تحت شبکه مورد نیاز است و در محل ذخیره سازی ممیزی، ذخیره می شود.

داده های کاربری ذخیره شده: فایل های داده و اطلاعاتی هستند که توسط کاربر ایجاد و ذخیره می شوند. این داده ها می تواند شامل مستندات تولید شده با استفاده از برنامه کاربردی Microsoft Office، نامه های ارجاع کار و پاسخ الکترونیکی و اسکن تصاویر باشد.

موجودیت فعال: موجودیتی در محصول که عملیاتی را بر روی موجودیت های غیرفعال انجام می دهد. همانند نقش هایی همچون مدیر، کاربر نهایی و غیره.

موجودیت غیرفعال: موجودیتی در محصول، که حاوی اطلاعات است و یا اطلاعات را دریافت می نماید و توسط موجودیت های فعال، عملیاتی بر روی آن انجام می گیرد. همانند لیست کردن رکوردها توسط مدیر سیستم، حذف فایل ها توسط مهاجم. (رکوردها و فایل ها موجودیت های غیرفعال هستند).

مشخصه های موجودیت فعال: مشخصه های هر موجودیت فعال می تواند از قبیل نام کاربری، کلمه عبور، آدرس IP کاربر باشد.

مشخصه های موجودیت غیرفعال: مشخصه های هر موجودیت غیرفعال می تواند از قبیل نوع، نام و اندازه مستند باشد.

۳ شرح محصول

محصول مورد ارزیابی، برنامه کاربردی مبتنی بر شبکه است که برای مدیریت رکوردها و مستندات مورد استفاده قرار می‌گیرد. از جمله وظایف این برنامه‌های کاربردی می‌توان به جمع‌آوری، ذخیره و توزیع مستندات، پیام‌ها و فرم‌های ارتباطات اداری بین افراد اشاره نمود. بطور کلی برنامه کاربردی تحت شبکه برای رکوردها و مستندات الکترونیکی از فعالیت‌های زیر استفاده می‌کند:

- ثبت رکوردهای الکترونیکی
- مدیریت گردش کار رکوردهای الکترونیکی
- ایجاد و مدیریت فرآیندهای آرشیو
- انجام امور جستجو و گزارش دهی
- قابلیت مدیریت کاربران
- پشتیبانی از سازوکارهای امن‌سازی ارتباطات
- سازوکارهای احراز هویت و کنترل دسترسی

محصول اعمال فوق را با کمک مؤلفه های نشان داده شده در شکل ۱ انجام می دهد.



شکل ۱: مؤلفه های برنامه کاربردی تحت شبکه

۳,۱ مؤلفه‌های محیط عملیاتی

یک برنامه کاربردی تحت شبکه، یک برنامه اجرایی بر روی بستر شبکه می‌باشد و با مؤلفه‌های شبکه در تعامل است که بر روی سیستم عامل اجرایی در محیط شبکه اجرا می‌گردد. محصول با واحد/واحدهای ذخیره‌سازی به منظور نگهداری رکوردها و با مؤلفه‌های ممیزی به منظور نگهداری رکوردهای ممیزی در تعامل است؛ در ادامه، این مؤلفه‌ها با جزئیات شرح داده می‌شوند.

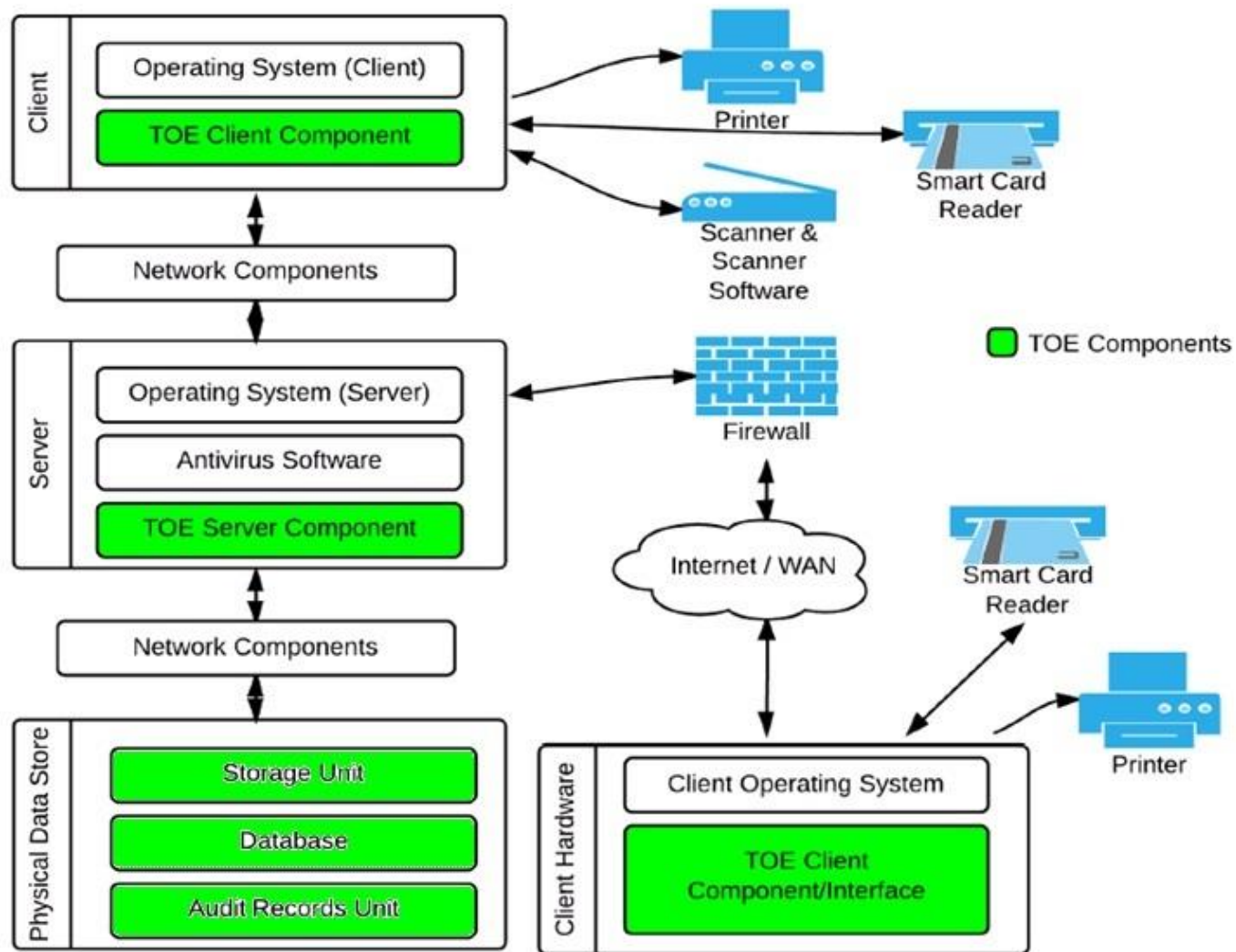
محیط عملیاتی محصول شامل مؤلفه‌های نرم‌افزاری و سخت‌افزاری و همچنین ویژگی‌های کارکردی و امنیتی اصلی می‌باشد که در این سند پوشش داده شده‌اند. شکل ۲ بیانگر سخت‌افزار و نرم‌افزارهایی است که محصول با آنها در تعامل می‌باشد، این شکل چگونگی تعاملات محصول با محیط عملیاتی را نمایش می‌دهد:

سرور: سرور مؤلفه سخت‌افزاری است که مؤلفه سروری محصول بر روی آن اجرا می‌گردد. سرور می‌تواند به صورت فیزیکی یا مجازی باشد، در هر دو حالت امنیت سرور به امنیت محصول بستگی دارد. پیکربندی و قابلیت‌های سرور می‌تواند با توجه به تعداد کاربران، تعداد اتصالات و غیره متفاوت باشد.

سیستم کاربر: سخت‌افزار و سیستم عاملی است که به کاربران اجازه دسترسی به محصول را می‌دهد. این مؤلفه معمولاً یک کامپیوتر بوده ولی می‌تواند یک تبلت یا گوشی هوشمند نیز باشد، در این پروفایل حفاظتی فرض شده که کلاینت یک کامپیوتر است. دو نوع کلاینت وجود دارد. یکی برای کاربر پایانی و نوع دیگر برای کاربرانی که رکوردها و مستندات را به داخل محصول وارد می‌نمایند. اتصالات بین کلاینت‌ها و مؤلفه‌های مرکزی محصول می‌تواند به صورت اینترنت، اینترنت یا VPN باشد.

سیستم عامل: محصول بر روی یک سیستم عامل اجرا می‌شود و ارتباطات بین محصول و واحد ذخیره‌سازی، واحد رکوردهای ممیزی، مؤلفه‌های شبکه و سرور توسط سیستم عامل ارائه می‌شود.

مؤلفه‌های شبکه: محصول به واسطه سیستم عامل و سرور با مؤلفه‌های شبکه در تعامل می‌باشد. لازم است اتصالات شبکه بین کلاینت‌ها و سرور محصول به صورت امن باشد. کلاینت محصول قادر به انجام اقداماتی همانند چاپ، اسکن و غیره است. اتصالات بین این مؤلفه‌ها و سرور معمولاً به صورت یک شبکه محلی می‌باشد.



شکل ۲: محیط عملیاتی محصول

فایروال: دسترسی اینترنت بوسیله‌ی این مؤلفه امن می‌گردد.

نرم‌افزار آنتی ویروس: نرم‌افزار آنتی ویروس جهت بررسی مستندات و رکوردهای ورودی مورد استفاده قرار می‌گیرد.

پایگاه داده: محصول با یک پایگاه داده برای حفظ و نگهداری داده‌های خود در تعامل نزدیک است. رکوردها و مستندات می‌توانند در پایگاه داده یا به صورت مجزا حفظ و نگهداری شوند. در زمان نیاز به یک مجموعه داده خاص، یک درخواست به پایگاه داده ارسال و نتایج آن گرفته می‌شود.

واحد ذخیره‌سازی مستندات و رکوردها: رکوردها و مستندات می‌توانند به صورت مجزا در سمت سروری که محصول بر روی آن اجرا می‌گردد باقی مانده تا محصول به آسانی تحت تاثیر آسیب‌پذیری امنیتی بالقوه در واحد ذخیره‌سازی قرار نگیرد.

واحد ذخیره رکوردهای ممیزی: همانند واحدهای ذخیره‌سازی، واحد رکوردهای ممیزی در سمت سروری قرار می‌گیرد که محصول بر روی آن اجرا می‌گردد. این واحد می‌تواند به صورت مؤلفه مجزا و یا بخشی از واحد ذخیره‌سازی باشد.

کارتخوان هوشمند: کارتخوان یک مؤلفه سخت‌افزاری است که دارای گواهی مورد اعتماد می‌باشد و برای امضاء اسناد الکترونیکی مورد استفاده قرار می‌گیرد. در حال حاضر رایج‌ترین نوع کارتخوان توکن USB می‌باشد. از آنجائیکه این مؤلفه مبتنی بر سخت‌افزار بوده و به شبکه متصل نمی‌باشد، سطح بالایی از امنیت را فراهم می‌نماید. از اینرو می‌تواند برای احراز هویت مورد استفاده قرار گیرد.

اسکنر و درایور آن: کاربرانی که برای اسکن نمودن مجاز هستند، رکوردها و مستنداتی که به شکل کاغذی دریافت می‌کنند را اسکن می‌نمایند.

پرینتر: مؤلفه‌ای است که به کاربران محصول مطابق با مجوز کاربر، اجازه چاپ هر رکورد یا مستندی را می‌دهند.

۳,۲ انواع کاربران

حداقل دو دسته کاربر برای محصول وجود دارد:

- کاربر عادی
- مدیر سیستم

علاوه بر نقش های لیست شده در بالا، محصول ممکن است دارای نقش های دیگری نیز باشد. در صورت وجود نقش های دیگر لازم است در سند هدف امنیتی ذکر گردد.

کاربر عادی: کاربر عادی از محصول به صورت یک جعبه سیاه استفاده می نماید و نیز قادر به مدیریت داده های تحت مالکیتش می باشد. کاربر عادی در صورت داشتن مجوز می تواند رکوردها و مستندات را جستجو، لیست و مشاهده نماید. علاوه بر آن کاربر عادی می تواند سند یا رکورد جدیدی ایجاد نماید یا سند و رکوردی که مالک آن است را حذف نماید. این نوع کاربر می تواند مستندات را بایگانی نماید و باید قادر به دسترسی اسناد بایگانی شده خود باشد.

مدیر سیستم: مدیر، دارای مجوز خاص برای مدیریت محصول می باشد. مدیر سیستم می تواند یک نفر باشد یا برای بخش های مختلف محصول مدیران مختلفی وجود داشته باشد، همانند مدیر پایگاه داده، مدیر شبکه، مدیر برنامه کاربردی و غیره. همچنین مدیر دارای سطح دسترسی کامل برای دسترسی به برنامه کاربردی، پایگاه داده، فایل سیستم و دیگر موجودیت ها می باشد.

۳,۳ ویژگی های امنیتی محصول

احراز هویت و مجوزدهی: عملیات احراز هویت و مجوزدهی باید به طور موثری انجام شود. احراز هویت به طور کلی با بررسی و تائید نام کاربری و کلمه عبور صورت می گیرد. لازم به ذکر است برای مدیریت کلمه عبورهای مورد استفاده باید روال های امن وجود داشته باشد. در صورتیکه محصول به سطح بالایی از امنیت نیاز داشته باشد، از یک سازوکار احراز هویت دیگر یا ترکیبی از دو یا بیشتر از دو سازوکار استفاده می شود. از جمله سازوکارهای احراز هویت می توان به واری نام کاربری و کلمه عبور، واری SMS، احراز هویت از طریق یک برنامه موبایل، گواهی دیجیتال، واری بیومتریک و توکن سخت افزاری اشاره نمود.

کنترل دسترسی: محصول، قابلیت‌های لازم برای محدود کردن دسترسی را دارد، بطوریکه تنها موجودیت‌های مجاز، دارای دسترسی به داده و کارکردهای محصول هستند. برای کاربران مجاز، کنترل دسترسی معمولاً با استفاده از داده احراز هویت انجام می‌گیرد. محصول ممکن است همچنین آدرس‌های IP اتصالات فعال را کنترل نماید، و تنها به آدرس‌های IP از پیش تعریف شده در یک بازه زمانی خاص برای عملیات‌های حساس اجازه اتصال دهد.

ممیزی: محصول به صورت خودکار، رکوردهای ممیزی را به منظور ردیابی و کنترل فعالیت‌های کاربر بر روی دارایی‌ها، تغییرات کنترل دسترسی و پیکربندی جمع‌آوری می‌نماید. محتوای رکوردهای ممیزی، روش‌های حفظ رکورد و فواصل نگهداری را می‌توان توسط رابط گرافیکی محصول پیکربندی نمود. هیچ فردی جز افرادی که محصول، مجاز نموده همچون مدیر، امکان تغییر یا حذف محتویات رکوردهای ممیزی را ندارند.

مدیریت: محصول، برای مدیریت کاربران و دسترسی‌ها واسط‌های مدیریتی لازم را فراهم می‌نماید. سرعت و دقت این واسط‌ها در تصمیم‌گیری در طول یک رخداد امنیتی بسیار مهم است.

صحت رکوردها و بررسی منابع: حذف یا تغییر هر رکورد توسط محصول مجاز نمی‌باشد. بنابراین، دسترسی و تغییر سند و/یا فرا داده^۱ آن باید محدود گردد. صحت رکوردهای ذخیره شده، توسط روشی مانند امضای دیجیتال مهیا می‌گردد.

پشتیبان‌گیری: عملیات پشتیبان‌گیری بر روی داده، مستندات و رکوردهای ممیزی که محصول از آنها محافظت می‌نماید، می‌تواند توسط خود محصول و یا یک ابزار خارجی که بدین منظور استفاده می‌گردد، صورت گیرد. عملیات پشتیبان نسبت به عدم از دست رفتن داده اطمینان می‌دهد.

کنترل گردش مستندات و اطلاعات: حداکثر اندازه فایل می‌تواند به صورت پویا برای هر نوع سند تعریف شود. محصول، فضای خالی ذخیره سازی را در نظر گرفته و در برابر سرریز ذخیره‌سازی اقدامات احتیاطی لازم را اتخاذ می‌نماید. همچنین تنها کاربران مجاز، مجوز صدور و ارسال هر رکورد یا سندی را دارند.

^۱ MetaData

درهم‌سازی/رمز نمودن داده حساس: مثالی از داده حساس کلمه‌های عبور یا رکوردهای محرمانه می‌باشد. داده حساس بر روی محصول به صورت واضح ذخیره نمی‌شوند و با سازوکاری از آنها حفاظت می‌شود. همچنین باید رکوردهای محرمانه به صورت رمز شده نگهداری شود. ارتباط بین کاربر و سرور باید با استفاده از رمزنگاری امن شود تا از افشای محتوی رکوردها جلوگیری گردد. روش درهم‌سازی و رمزنگاری انتخاب شده باید به اندازه کافی قوی باشد طوری که توسط فناوری‌های امروزی در یک بازه‌ی منطقی قابل شکسته شدن نباشد.

۴ مسائل امنیتی

۴,۱ تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم می‌تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی می‌تواند با استفاده از هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد. مهاجم می‌تواند با سود بردن از نقض‌های امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری آزمون بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم می‌تواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده‌های می‌توانند داده‌های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم می‌تواند با دسترسی به داده‌ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردهای، مستندات و داده‌های حفاظت شده توسط محصول می‌تواند بدون مجوز تغییر یابند. مهاجم می‌تواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می‌تواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده‌های حفاظت شده توسط

توضیحات	تهدیدات
محصول را تغییر دهد. این تهدید زمانی رخ می‌دهد که صحت رکوردها و مستندات تضمین شده نمی‌باشد. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.	
یک اقدام یا یک تراکنش صورت گرفته بر روی محصول می‌تواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول می‌باشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می‌تواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم می‌تواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.	انکار
داده‌های محرمانه که توسط محصول محافظت می‌شوند می‌تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می‌تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی می‌تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده می‌تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.	افشای اطلاعات
مهاجم می‌تواند سبب گردد محصول در یک بازه زمانی غیر قابل دسترسی یا بلا استفاده گردد. این امر معمولاً با ارسال درخواست‌های بسیار در یک بازه زمانی کوتاه صورت می‌گیرد طوری که محصول قادر به پاسخ نخواهد بود. نوع ساده‌ای از حمله شامل ارسال درخواست‌های بسیار از یک رنج IP مشخص می‌باشد که به نام حمله DoS شناخته می‌شود. نوع دیگر پیشرفته‌تر حمله DDOS می‌باشد که از BOTNET استفاده می‌نماید و محدودیتی بر روی آدرس IP ورودی ندارد.	انکار سرویس
مهاجم می‌تواند یک رکورد، سند یا داده مضر را در داخل محصول وارد نماید. با استفاده از این تهدید، مهاجم می‌تواند به داده کاربر خاص دسترسی پیدا نماید، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.	داده‌های ورودی مخرب

توضیحات	تهدیدات
مهاجم می تواند با سود بردن از دسترسی غیرمجاز، ورود داده های مخرب و تغییر داده ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.	سطح دسترسی بالاتر
در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می شود تا انتقال داده های حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده های رد و بدل شده بین محصول و یک یا چند کاربر از راه دور و یا محلی است. به عنوان مثال می توان به موردی اشاره کرد که در آن یک کاربر تلاش می کند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد می نماید.	شنود شبکه

۴,۲ خط مشی امنیتی

توضیحات	خط مشی ها
تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار می گیرند.	ممیزی کامل
پیکربندی پیش فرض محصول و مؤلفه های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس هایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیش فرض، خطاهای پیش فرض و صفحات 404، مقادیر احراز هویت پیش فرض، نام کاربری پیش فرض، پورتهای پیش فرض، صفحات پیش فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می نمایند. این خط مشی سازمانی بسیار مهم است به خصوص زمانی که محصول یا هر مؤلفه تعاملی به طور گسترده مورد استفاده قرار می گیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی می توان از حمله ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.	پیکربندی مناسب

خط مشی ها	توضیحات
امضای دیجیتال	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تأیید موجود باشد.

۴,۳ فرضیات

فرضیات	توضیحات
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده اند و قوانین را دنبال می نمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می نمایند.
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب پذیری های شناخته شده را اتخاذ می نمایند.
محیط امن	فرض شده است که تمام پیش بینی های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیر قانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدامات مناسبی صورت می گیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره سازی و دیگر مؤلفه های سخت افزاری دارای پشتیبان مناسبی هستند، و بنابر وجود نسخه پشتیبان هیچ داده ای از دست نمی رود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمی دهد.

توضیحات	فرضیات
فرض شده است که تمام ارتباطات و کانال‌های ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی در قبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می‌شوند.	ارتباطات
فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت می‌گیرد.	تحویل امن
فرض شده است که اقدامات امنیتی لازم در قبال حملات DDOS اتخاذ می‌شود.	انکار سرویس توزیع شده

۵ اهداف امنیتی

۵,۱ اهداف امنیتی برای محصول

توضیحات	هدف امنیتی
محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش رکورد نماید. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت نماید. محصول باید به کاربران مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به موقع از رخداد امنیتی بحرانی آگاه نماید.	ممیزی

توضیحات	هدف امنیتی
محصول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصول باید برای احراز هویت کاربر، قوانینی تعریف نماید طوریکه کاربران را ملزم به استفاده از کلمه های عبور قدرتمند نماید. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف نماید. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم می نماید. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم نماید. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید با استفاده از سازوکارهای قویتری مدیر سیستم را احراز هویت نماید. از جمله سازوکارها می توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احراز هویت براساس توکن، احراز هویت چند فاکتوری و ترکیبی از این روش ها اشاره نمود.	احراز هویت
محصول باید گردش داده های غیرمجاز را کنترل و مدیریت نماید. داده های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست ها از یک رنج IP تعریف شده می تواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.	کنترل جریان داده
محصول باید نسبت به صحت داده ممیزی و داده ی رکورد با تشخیص هرگونه تغییر بر روی این داده ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.	صحت داده

توضیحات	هدف امنیتی
محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارآمد سیستم فراهم نماید. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسطه‌های مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقش‌های کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقش‌ها و مجوزهایی تنظیم نماید.	مدیریت
محصول باید صورت امن و کارآمد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات جزئی چون شماره خط برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید.	مدیریت خطا
محصول باید اطمینان دهد که هر داده‌ی باقیمانده از محصول زمانی که دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترسی می‌گردد.	مدیریت داده‌های باقیمانده
تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.	ارتباطات امن مبتنی بر TLS

۵,۲ اهداف امنیتی برای محیط عملیاتی

اهداف امنیتی محیطی	توضیحات
محیط امن	محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام مؤلفه‌ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مؤلفه‌های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظت شده است. از جمله سازوکارهای حفاظتی می‌توان به غیرفعال نمودن سرویس‌ها، پورت‌ها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌های ارتباطی امن باید فراهم گردد.
کاربران آموزش دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته شده را در نظر می‌گیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مؤلفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول می‌باشد. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود.
تحویل امن	تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. علاوه بر این، کارکردها و/یا پارامترهای استفاده شده به منظور آزمون باید پاک یا غیر قابل دسترس گردند.

اهداف امنیتی محیطی	توضیحات
پشتیبان گیری مناسب	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده های باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روال های از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مؤلفه های سخت افزاری نیز نسخه پشتیبان تهیه گردد.

۶ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده شده اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	تولید داده ممیزی ۱	FAU_GEN.1.1
۲	تولید داده ممیزی ۲	FAU_GEN.1.2
۳	مرتبط نمودن هویت کاربر به رویداد ۱	FAU_GEN.2.1
۴	بازبینی داده ممیزی ۱	FAU_SAR.1.1
۵	بازبینی داده ممیزی ۲	FAU_SAR.1.2
۶	بازبینی داده ممیزی محدود ۱	FAU_SAR.2.1
۷	بازبینی داده ممیزی قابل انتخاب ۱	FAU_SAR.3.1
۸	ذخیره سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۹	ذخیره سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۱۰	اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	FAU_STG.3.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۱	پیشگیری از ائتلاف و از بین رفتن داده‌های ممیزی ۱	FAU_STG.4.1
۱۲	انتخاب داده ممیزی ۱	FAU_SEL.1.1
۱۳	عملیات رمزنگاری ۱(۱)	FCS_COP.1.1(1)
۱۴	عملیات رمزنگاری ۱(۲)	FCS_COP.1.1(2)
۱۵	مدیریت کلمه عبور	FIA_PMG_EXT.1.1
۱۶	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۱۷	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۱۸	تعریف مشخصات کاربر ۱	FIA_ATD.1.1
۱۹	شناسایی کاربر ۱	FIA_UID.1.1
۲۰	شناسایی کاربر ۲	FIA_UID.1.2
۲۱	احراز هویت کاربر ۱	FIA_UAU.1.1
۲۲	احراز هویت کاربر ۲	FIA_UAU.1.2
۲۳	سازوکار احراز هویت چندگانه ۱	FIA_UAU.5.1
۲۴	سازوکار احراز هویت چندگانه ۲	FIA_UAU.5.۲
۲۵	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱	FIA_USB.1.1
۲۶	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.1.2
۲۷	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.1.۳
۲۸	حفاظت کامل از اطلاعات باقیمانده در منابع ۱	FDP_RIP.2.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۲۹	ورود داده های کاربری به محصول با مشخصه امنیتی ۱	FDP_ITC.2.1
۳۰	ورود داده های کاربری به محصول با مشخصه امنیتی ۲	FDP_ITC.2.2
۳۱	ورود داده های کاربری به محصول با مشخصه امنیتی ۳	FDP_ITC.2.3
۳۲	ورود داده های کاربری به محصول با مشخصه امنیتی ۴	FDP_ITC.2.۴
۳۳	ورود داده های کاربری به محصول با مشخصه امنیتی ۵	FDP_ITC.2.۵
۳۴	خروج داده های کاربری از محصول با مشخصه امنیتی ۱	FDP_ETC.2.1
۳۵	خروج داده های کاربری از محصول با مشخصه امنیتی ۲	FDP_ETC.2.۲
۳۶	خروج داده های کاربری از محصول با مشخصه امنیتی ۳	FDP_ETC.2.۳
۳۷	خروج داده های کاربری از محصول با مشخصه امنیتی ۴	FDP_ETC.2.۴
۳۸	صحت داده های کاربری ذخیره شده ۲	FDP_SDI.2.1
۳۹	صحت داده های کاربری ذخیره شده ۳	FDP_SDI.2.2
۴۰	خط مشی کنترل دسترسی ۱	FDP_ACC.1.1
۴۱	عملیات کنترل دسترسی ۱	FDP_ACF.1.1
۴۲	عملیات کنترل دسترسی ۲	FDP_ACF.1.2
۴۳	عملیات کنترل دسترسی ۳	FDP_ACF.1.3
۴۴	عملیات کنترل دسترسی ۴	FDP_ACF.1.۴
۴۵	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
۴۶	مدیریت مشخصه های امنیتی ۱	FMT_MSA.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۷	مقداردهی اولیه مشخصه ها ۱	FMT_MSA.3.1
۴۸	مقداردهی اولیه مشخصه ها ۲	FMT_MSA.3.2
۴۹	مدیریت داده های محصول ۱-مدیر سیستم	FMT_MTD.1.1(1)
۵۰	مدیریت داده های محصول ۱-کاربر عادی، وارد کننده داده	FMT_MTD.1.1(2)
۵۱	کارکردهای مدیریتی محصول ۱	FMT_SMF.1.1
۵۲	نقش های امنیتی ۱	FMT_SMR.1.1
۵۳	نقش های امنیتی ۲	FMT_SMR.1.2
۵۴	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۵۵	سازگاری داده های امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.1.1
۵۶	سازگاری داده های امنیتی بین محصول و موجودیت امن ۲	FPT_TDC.1.۲
۵۷	انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۵۸	مهرهای زمانی ۱	FPT_STM.1.1
۵۹	به روز رسانی امن ۲	FPT_TUD_EXT.1.2
۶۰	به روز رسانی امن ۳	FPT_TUD_EXT.1.3
۶۱	محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.1.1
۶۲	محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.1.2
۶۳	خاتمه دادن به نشست ها توسط محصول ۱	FTA_SSL.3.1
۶۴	خاتمه دادن به نشست ها توسط کاربر ۱	FTA_SSL.4.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۶۵	سوابق دسترسی به محصول ۱	FTA_TAH.1.1
۶۶	سوابق دسترسی به محصول ۲	FTA_TAH.1.۲
۶۷	سوابق دسترسی به محصول ۳	FTA_TAH.1.۳
۶۸	برقراری نشست ۱	FTA_TSE.1.1
۶۹	تحمل خطا ۱	FRU_FLT.1.1
۷۰	مسیر امن ۱	FTP_TRP.1.1
۷۱	مسیر امن ۲	FTP_TRP.1.2
۷۲	مسیر امن ۳	FTP_TRP.1.3
الزامات پیوست یک		
۷۳	تولید کلید رمزنگاری ۱	FCS_CKM.۱.۱
۷۴	تخریب کلید رمزنگاری ۱	FCS_CKM.۴.۱
۷۵	عملیات رمزنگاری ۱- رمزگشایی ۱(۳)	FCS_COP.۱.۱(۳)
۷۶	عملیات رمزنگاری ۱(۴)	FCS_COP.۱.۱(۴)
الزامات پیوست دو		
۷۷	الزامات پروتکل TLS Server / احراز هویت ۱	FCS_TLSS_EXT.1.1
۷۸	الزامات پروتکل TLS Server / احراز هویت ۲	FCS_TLSS_EXT.1.2
۷۹	الزامات پروتکل TLS Server / احراز هویت ۳	FCS_TLSS_EXT.1.3

۶,۱ کلاس ممیزی امنیت

شماره الزام	نام الزام	
۱	تولید داده ممیزی ۱	
محصول باید براساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید: • آغاز و اتمام توابع ممیزی؛ • تمامی رویدادهای قابل ممیزی (برای نوع داده حساس و داده هایی که بار حقوقی دارند) که در جدول ۱ آمده است. جدول ۱- لیست رویدادهای قابل ممیزی		
مؤلفه	رویداد قابل ممیزی	جزئیات
مرتبط نمودن هویت کاربر به رویداد ۱	تلاش های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
بازبینی داده ممیزی ۱	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
انتخاب داده ممیزی ۱	ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می افتد در حالی که توابع ممیزی در حال انجام عملیات باشند. (حداقل)	
اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	عملیات انجام شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)	
پیشگیری از اتلاف و از بین رفتن داده های ممیزی ۱	عملیات انجام شده به دلیل شکست ذخیره سازی ممیزی (پایه)	

۲	صحت داده های کاربری ذخیره شده	تلاش های موفقیت آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاش ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)
	احراز هویت کاربر	ثبت کاربرد ناموفق از سازوکار احراز هویت (حداقل) ثبت تمام کاربردهای سازوکار احراز هویت (پایه)
	سازوکار احراز هویت چندگانه	ثبت نتایج احراز هویت (حداقل) ثبت هر سازوکار احراز هویت فعال همراه با نتیجه نهائی (پایه)
	شناسایی کاربر	شناسه کاربر شامل آدرس مبدا، شناسایی نقطه پایانی اتصال تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)
	مدیریت کلمه عبور	ثبت رد هر کلمه عبور آزمون شده توسط محصول (حداقل) ثبت تلاش موفق و ناموفق هر کلمه عبور آزمون شده توسط محصول (پایه)
	انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	ثبت شکست انقیاد مشخصه های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل) شکست و موفقیت انقیاد مشخصه های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه)
	مدیریت مشخصه های امنیتی	تمامی تغییرات بر روی مقادیر مشخصه های امنیتی (پایه)
	مدیریت داده های محصول ۱-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده های امنیتی محصول (پایه) به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
	مدیریت داده های محصول ۱- کاربر عادی، وارد کننده داده	تمامی تغییرات بر روی مقادیر داده های امنیتی محصول (پایه) به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
	عملیات رمزنگاری (۱)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل)

	هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	
	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	عملیات رمزنگاری ۱ (۲)
شناسایی داده‌های موجودیت غیرفعال	درخواست‌های موفقیت‌آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل) تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	عملیات کنترل دسترسی ۱
	ورود داده کاربری موفقیت‌آمیز، شامل هر گونه مشخصه‌های امنیتی (حداقل) تمامی تلاش‌ها برای وارد کردن داده‌های کاربری، شامل هر گونه مشخصه‌های امنیتی (پایه)	ورود داده‌های کاربری به محصول با مشخصه امنیتی
	خروج اطلاعات به‌طور موفقیت‌آمیز (حداقل) همه تلاش‌ها برای خارج کردن اطلاعات از محصول (پایه)	خروج داده‌های کاربری از محصول با مشخصه امنیتی
	تمامی تغییرات در رفتارهای کارکردی محصول	مدیریت کارکرد در محصول
	ثبت استفاده از کارکردهای مدیریتی (حداقل)	کارکردهای مدیریتی محصول
	ثبت تغییرات در گروه‌های کاربری که بخشی از یک نقش می‌باشد (حداقل)	نقش‌های امنیتی
	ثبت استفاده موفق از مکانیزم سازگاری داده‌های محصول (حداقل) ثبت استفاده از مکانیزم سازگاری داده‌های محصول (پایه)	سازگاری داده‌های امنیتی بین محصول و موجودیت امن
	ثبت شکست در محصول (پایه)	حفظ وضعیت امن در زمان شکست
	ثبت هر شکست شناسایی شده توسط محصول (حداقل)	تحمل خطا

	ثبت تمامی قابلیت های در حال قطع شدن محصول که به دلیل شکست می باشد (پایه)	
برقراری نشست ۱	ثبت منع آغاز نشست بدلیل مکانیزم آغاز نشست (حداقل) ثبت تمامی تلاش ها در آغاز نشست کاربر (پایه)	
محدودیت بر روی چندین نشست همزمان	ثبت رد یک نشست مبتنی بر محدودیت نشست های همزمان (حداقل)	
خاتمه دادن به نشست ها	ثبت خاتمه دادن به یک نشست بیکار توسط مکانیزم قفل نشست (حداقل) ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)	

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول^۲**
توسعه گر محصول باید قالب و نحوه ذخیره سازی رکوردهای ممیزی را در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی بیان نماید و چگونگی استخراج رکوردهای ممیزی توسط مدیر سیستم و یا ارزیاب به منظور تحلیل داده ها، توضیح داده شود.
- **سند راهنمای محصول**
ارزیاب باید سند راهنمای محصول را بررسی نماید تا نسبت به ارائه لیستی از رویدادهای قابل ممیزی در محل ذخیره سازی به شکل مناسب و قابل درک اطمینان حاصل نماید.
- **آزمون ها**
ارزیاب باید آزمون های زیر را برای هر کدام از انواع رویدادها انجام دهد:

^۲ TOE Summory Specification (TSS)

آزمون اول: ارزیاب باید نشستی را با سرور ایجاد و درخواستی به آن ارسال نماید. سپس باید تولید لاگ در سرور برای درخواست ارسال شده را بررسی نماید. آزمون دوم: ارزیاب باید عملیاتی را انجام دهد که منجر به ثبت هر کدام از رویدادهای قابل ممیزی می شود. سپس ثبت و یا عدم ثبت آنها را بررسی نماید. آزمون سوم: ارزیاب باید با انجام یک عمل غیر مجاز، عدم تولید لاگ در سرور را بررسی نماید.	
۲	تولید داده ممیزی ۲
محصول باید برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید: • تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال (در صورتی که کاربرد داشته باشد) و نتیجه (موفقیت یا شکست) رویداد • [اختصاص: هر نوع اطلاعات قابل ممیزی دیگر از قبیل آدرس IP کاربر، نام و شناسه کاربری، نسخه سیستم عامل، زمان و تاریخ انجام فعالیت.] اقدامات ارزیابی: • سند راهنمای محصول ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید در سند مذکور، نحوه نمایش لاگ های ممیزی ذخیره شده در شکل و فرمت مناسب شرح داده شده است. • آزمون ها ارزیاب باید بررسی کند برای لاگ ثبت شده در سرور، اطلاعات ذکر شده در این الزام وجود دارد یا خیر.	
۳	مرتبط نمودن هویت کاربر به رویداد ۱

برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی شده، محصول باید بتواند هویت کاربری که باعث ایجاد آن رویداد شده است، را شناسایی و ثبت نماید.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول**

در این بخش باید در صورت امکان روش‌هایی که باعث عدم انقیاد رویداد مرتبط با کاربری که آن را ایجاد کرده است، توضیح داده شود.

- **آزمون**

آزمون این الزام وابسته به الزام شماره ۱ «تولید داده ممیزی ۱» است. ارزیاب باید رکوردهای ممیزی تولید شده را مطابقت دهد که آیا به نام همان کاربری که آن رویداد را ایجاد کرده، ذخیره شده است؟

۴	بازبینی داده ممیزی ۱
---	----------------------

محصول باید امکان خواندن/مشاهده [اختصاص: فهرستی از اطلاعات ممیزی] از کل رکوردهای ممیزی را برای [اختصاص: کاربران مجاز] فراهم نماید.

نکته کاربردی ۲:

- به جای کاربران مجاز، با توجه به سازوکار کنترل دسترسی در محصول، کاربران و یا گروه کاربرانی که مجاز به قابلیت خواندن اطلاعات ممیزی هستند را اعلام نماید.

- به جای فهرستی از اطلاعات ممیزی، با توجه به سازوکار کنترل دسترسی در محصول، نوع اطلاعات ممیزی که کاربر مجاز قابلیت خواندن آنها را دارد را اعلام نمایید.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول**

در این بخش از سند هدف امنیتی باید توضیح داده شود که چه مواقعی کاربر قادر به خواندن داده ممیزی است.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و تأیید نماید چه زمانی برای کاربر امکان خواندن رکورد ممیزی داده می‌شود و کدام واسطه‌هایی این امکان را فراهم می‌کنند.

ارزیاب باید با بررسی سند راهنمای محصول تأیید نماید که در این سند در خصوص زمانی که کاربر امکان خواندن رکورد ممیزی دارد و از طریق کدام واسطه‌ها این امکان فراهم می‌شود توضیحاتی ارائه شده است.

• آزمون‌ها

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که تنها کاربر با دسترسی مجاز قادر به خواندن رکوردهای ممیزی در فرمت مناسب و قابل درک است.
آزمون دوم: ارزیاب باید بررسی کند که با توجه به نوع دسترسی کاربران، اطلاعات و رکوردهای ممیزی مناسب و خاص خود را قادر به خواندن هستند.

۵	بازبینی داده ممیزی ۲
---	----------------------

محصول باید رکوردهای ممیزی را به شکل خوانا و قابل درک برای کاربر نمایش دهد.

اقدامات ارزیابی:

آزمون این الزام وابسته به الزام شماره ۴ «بازبینی ممیزی امنیت ۱» است.

۶	بازبینی داده ممیزی محدود ۱
---	----------------------------

محصول باید مانع دسترسی خواندن رکوردهای ممیزی توسط کلیه کاربران به غیر از کاربرانی که مجاز به دسترسی هستند (الزام شماره ۴ «بازبینی داده ممیزی ۱»)، شود.

اقدامات ارزیابی:

• سند راهنمای محصول

ارزیاب باید سند راهنمای محصول را بررسی و تأیید نماید چه زمانی برای کاربر امکان خواندن رکورد ممیزی داده می‌شود و کدام واسطه‌ها این امکان را فراهم می‌کنند.

آزمون‌ها ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به خواندن رکوردهای ممیزی است یا خیر.	
۷	بازبینی داده ممیزی قابل انتخاب ۱
آزمون‌ها ارزیاب باید بتواند بر اساس یکی از داده‌های ممیزی، مرتب‌سازی نماید.	محصول باید امکان انجام [اختصاص: متدهای انتخاب و مرتب سازی] رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را براساس [اختصاص: حساب کاربری، تاریخ/زمان، نوع رخداد و دیگر پارامترهای مورد نیاز] مرتب نماید. اقدامات ارزیابی: راهنما ارزیاب باید سند راهنمای محصول را بررسی کند که نحوه مرتب‌سازی داده‌های ممیزی بیان شده است و کدام واسط‌ها این امکان را فراهم می‌کنند.
۸	ذخیره سازی رویدادهای ممیزی ۱

محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را، از حذف غیرمجاز حفاظت نماید.

اقدامات ارزیابی:

- خلاصه مشخصات محصول

ارزیاب باید اطمینان حاصل نماید که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی، مقدار حجم ذخیره سازی رکوردهای ممیزی به صورت محلی بیان شده است.

- سند راهنمای محصول

ارزیاب باید سند راهنمای محصول را بررسی نماید تا در خصوص بیان رابطه بین رکوردهای ممیزی محلی و رکوردهای ممیزی ارسالی به لاگ سرور اطمینان حاصل نماید. برای مثال، اگر رکورد ممیزی تولید شده باشد، به طور همزمان هم در سرور خارجی و هم در محل ذخیره سازی محلی ذخیره شود، یا محل ذخیره سازی محلی به عنوان بافر مورد استفاده قرار گیرد و با ارسال داده ها به طور دوره ای به سرور ممیزی، داده ها از محل ذخیره سازی محلی پاک گردد.

۹ ذخیره سازی رویدادهای ممیزی ۲

محصول باید قادر به [انتخاب : تشخیص، جلوگیری] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره سازی آنها باشد.

اقدامات ارزیابی:

- سند راهنمای محصول

ارزیاب باید سند راهنمای محصول را بررسی کند و درخصوص بیان اینکه چه زمانی برای کاربر امکان حذف و یا تغییر رکورد ممیزی داده می شود و کدام واسط این امکان را فراهم می کند اطمینان حاصل نماید.

- آزمون ها

ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به تغییر و یا حذف رکوردهای ممیزی است یا خیر. آزمون دوم: ارزیاب باید بررسی کند که در صورت تلاش کاربر غیرمجاز برای حذف و یا اعمال تغییرات بر روی رکوردهای ممیزی، در لاگ ذخیره شود.	
۱۰	اقدامات لازم در زمان از دست رفتن داده ممیزی ۱ محصول در صورت تجاوز دنباله ممیزی از [اختصاص: یک محدودیت از پیش تعریف شده] باید با استفاده از [اختصاص: یک کانال ارتباطی، پیام کوتاه یا معادل آن، از طریق واسطه‌های محصول کاربران مربوطه را] مطلع نماید. اقدامات ارزیابی: • خلاصه مشخصات محصول ارزیاب باید اطمینان حاصل نماید که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی مقدار حجم ذخیره‌سازی رکوردهای ممیزی به صورت محلی بیان شده است. همچنین نوع رویدادی که در صورت پر شدن محل ذخیره سازی رخ می‌دهد و چگونگی محافظت از رکوردهای ممیزی در برابر دسترسی‌های غیر مجاز مشخص گردد. در این بخش، عملیاتی که بعد از پر شدن محل ذخیره‌سازی ممیزی صورت می‌گیرد و نوع اطلاعاتی که ممکن است از بین رود باید بیان شود. همچنین نوع تنظیماتی که مدیر سیستم باید بر روی محصول پیکربندی کند تا عملیات مورد نظر فعال گردند، باید در این سند تعریف شود. • سند راهنمای محصول ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل نماید که توضیحاتی در خصوص رویدادهایی که برای پیشگیری از دست رفتن رکوردهای ممیزی در صورت پر شدن محل ذخیره‌سازی در نظر گرفته شده، بیان شده است. ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید که در خصوص رابطه بین رکوردهای ممیزی محلی و رکوردهای ممیزی ارسالی به لاگ سرور ممیزی توضیحاتی بیان شده باشد. برای مثال، اگر رکورد ممیزی تولید شده باشد، به‌طور همزمان هم در سرور خارجی و هم در

محل ذخیره‌سازی محلی ذخیره شود، یا محل ذخیره‌سازی محلی به عنوان بافر مورد استفاده قرار گیرد و با ارسال داده‌ها به طور دوره‌ای به سرور ممیزی، داده‌ها از محل ذخیره‌سازی محلی پاک گردد. • آزمون‌ها ارزیاب باید مقدار حد آستانه ذخیره‌سازی رکورد ممیزی را به گونه‌ای انتخاب نماید که محل ذخیره‌سازی پر شود و بررسی نماید که در این شرایط رویدادهای ادعا شده صورت می‌گیرد.	
۱۱	پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۱
محصول در صورت پر شدن دنباله ممیزی، باید [انتخاب: «رویدادهای ممیزی را نادیده بگیرد»، «از ذخیره رویدادهای قابل ممیزی، به جز آنهایی که توسط کاربر مجاز و تحت حقوق خاص رخ می‌دهند، جلوگیری نماید»، «روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده دوباره‌نویسی نماید»] و [اختصاص: یا دیگر اقدامات برای هشدار از پر شدن فضای ذخیره‌سازی] ارسال نمایند.	
۱۲	انتخاب داده ممیزی ۱
محصول باید قادر به انتخاب مجموعه‌ای از رخدادها جهت ممیزی شدن، از مجموعه تمام رخدادهای قابل ممیزی براساس مشخصه‌های زیر باشد: • [انتخاب: هویت موجودیت فعال، نوع رخداد] • [اختصاص: معیارهای انتخاب دیگر بیان شوند] اقدامات ارزیابی: • سند راهنمای محصول ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید که لیستی از انواع رویدادها و خصیصه‌های قابل ممیزی وجود دارد که قابل انتخاب می‌باشند. • آزمون‌ها	

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید به ازاء هر خصیصه و رویدادی که در لیست آمده است قابل انتخاب بودنشان برای ممیزی را بررسی نماید.
آزمون دوم: ارزیاب باید چندین آیتم از لیست را برای ممیزی انتخاب نموده و بررسی نماید که با اضافه شدن چندین نوع خصیصه و رویداد، عمل به‌درستی اجرا می‌شود.

۶,۲ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۳	عملیات رمزنگاری ۱ (۱)
محصول باید [اختصاص: برای واری صحت داده‌های ممیزی و داده‌های رکورد] بر اساس یک الگوریتم رمزنگاری مشخص [اختصاص: الگوریتم رمزنگاری] و اندازه کلید رمزنگاری [اختصاص: اندازه‌های کلید رمزنگاری] اجرا شود که مطابق با [اختصاص: لیستی از استانداردها] باشد. نکته کاربردی ۳: روش‌های اطمینان از صحت داده‌ی رکوردها و داده‌ی ممیزی بر عهده نویسنده سند هدف امنیتی می‌باشد. نویسنده در صورت استفاده از مؤلفه‌های اضافی به منظور صحت داده‌ها باید آنها را در سند هدف امنیتی اضافه نماید. ممکن است با توجه به روش بررسی صحت داده نیاز به الزامات ذکر شده در «پیوست یک» باشد. همچنین در صورت استفاده از کلید رمزنگاری در محصول لازم است نویسنده سند هدف امنیتی الزامات مرتبط را از پیوست انتخاب نموده و به صورت تکمیل شده در سند هدف امنیتی ذکر نماید.	
۱۴	عملیات رمزنگاری ۱ (۲)
محصول باید [اختصاص: تولید داده درهم‌سازی] بر اساس مجموعه الگوریتم‌های رمزنگاری مشخص [اختصاص: الگوریتم‌های رمزنگاری] و اندازه کلید رمزنگاری اختصاص: هیچکدام] اجرا شود که مطابق با [اختصاص: لیستی از استانداردها] باشد. نکته کاربردی ۴: از آنجائی که الگوریتم درهم‌سازی نیازی به کلید ندارد، محدودیتی برای اختصاص وجود ندارد.	

۶,۳ کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۱۵	مدیریت کلمه عبور
محصول باید قابلیت های مدیریت کلمه عبور را که در زیر ذکر شده اند برای کلمه عبورهای مدیریتی فراهم نماید: ۱. کلمه عبور باید بتواند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [انتخاب: "@", "#", "\$", "%", "^", "!", "&", "*", "(", ")"] باشد. ۲. حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و ۸ کاراکتر یا بیشتر باشد. نکته کاربردی ۵: نویسنده سند هدف امنیتی، کاراکترهای خاص پشتیبانی شده توسط محصول را انتخاب می نماید. نویسنده این اختیار را دارد تا کاراکترهای خاص بیشتری را با استفاده از عبارت «اختصاص» لیست نماید. «کلمه عبور مدیریتی» به آن دسته از کلمه عبورهای اشاره دارد، که مدیران از آنها در کنسول محلی یا پروتکل هایی که از «کلمه عبور» پشتیبانی می نمایند (همچون SSH, HTTPS)، استفاده می کنند. اقدامات ارزیابی: • سند راهنمای محصول ارزیاب باید راهنمای محصول را بررسی نموده تا اطمینان حاصل نماید در این سند توضیحات لازم در خصوص ایجاد کلمه عبورهای قوی و تنظیم طول کلمه عبور برای مدیران بیان شده است. • آزمون ها ارزیاب باید کلمه عبورهای ضعیف و قوی ایجاد نموده و عکس العمل محصول در خصوص پشتیبانی از هر دو کلمه عبور را بررسی نماید. ارزیاب باید اطمینان حاصل نماید که تمام کارکترها، قوانین و حداقل طول کلمه عبور که در سند راهنمای محصول آمده است پشتیبانی می گردد.	
۱۶	مدیریت احراز هویت ناموفق ۱

محصول، باید بتواند با استفاده از [انتخاب:] [اختصاص: یک عدد مثبت]، یک عدد مثبت قابل تنظیم توسط مدیر [اختصاص: بازه قابل قبولی از مقادیر] تلاش ناموفق احراز هویت مرتبط با [اختصاص: لیستی از رویدادهای احراز هویت] را تشخیص دهد.

نکته کاربردی ۶:

به عنوان مثال در سومین اختصاص می‌توان به وارد نمودن کلمه عبور توسط کاربر برای احراز هویت شدن اشاره نمود.

اقدامات ارزیابی:

• خلاصه مشخصات محصول

ارزیاب باید «خلاصه مشخصات محصول» از سند هدف امنیتی را بررسی نموده تا اطمینان حاصل نماید توضیحاتی در خصوص روش‌های مورد پشتیبانی برای عملیات مدیریتی از راه دور و چگونگی تشخیص تلاش‌های موفق و ناموفق احراز هویت ارائه شده است.

• سند راهنمای محصول

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل نماید توضیحاتی در خصوص دستورات پیکربندی تعداد تلاش‌های موفق و ناموفق احراز هویت، ارائه شده است و در صورت استفاده از روش‌های مختلف احراز هویت از راه دور همانند SSH باید در این سند شرح داده شود.

• آزمون‌ها

ارزیاب باید براساس حد آستانه تلاش موفق و ناموفق احراز هویت در راهنما، محصول را پیکربندی نماید و هنگامی که تعداد تلاش احراز هویت به مقدار حد آستانه رسید با نام کاربری و کلمه عبور معتبر احراز هویت را بررسی کند که در این صورت نباید اجازه ورود دهد.

۱۷	مدیریت احراز هویت ناموفق ۲
زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [انتخاب: به حد تعیین شده رسید، بیشتر از حد تعیین شده رسید]، محصول باید [اختصاص: لیستی از اقدامات مقابله‌ای] را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود. اقدامات ارزیابی: • سند راهنمای محصول	

ارزیاب باید سند راهنمای محصول را بررسی کند و اطمینان حاصل نماید، توضیحاتی در خصوص نحوه‌ی مدیریت احراز هویت در شرایطی که تعداد تلاش‌های ناموفق احراز هویت به بیش از حد آستانه (حد آستانه برای تلاش ناموفق نیز باید مشخص گردد) رسید ارائه شده باشد.	
۱۸	تعریف مشخصات کاربر ۱
محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید: [اختصاص: • شناسه کاربر • مدت احراز هویت مورد استفاده • داده‌های احراز هویت • نقش کاربر • وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره) • [اختصاص: هر مشخصه امنیتی دیگر]] نکته کاربردی ۷: حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باید وجود داشته باشد. این اطلاعات شامل نگهداری نمودن از هر مجوزی است که یک کاربر ممکن است دارا باشد. اقدامات ارزیابی: • خلاصه مشخصات محصول ارزیاب باید بررسی نماید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی مشخصه‌های امنیتی نگهداری شده برای هر کاربر تعریف شده باشد. البته ممکن است این لیست با لیست ذکر شده در الزام شماره ۱۸ «تعریف مشخصات کاربر ۱» متفاوت باشد. در این صورت، باید فصل «خلاصه مشخصات محصول» مشخصه‌های امنیتی مهم کاربر را پوشش دهد. • سند راهنمای محصول	

ارزیاب باید در راهنمای مدیریتی محصول از سند راهنما توضیحاتی در خصوص ایجاد، مشاهده، تغییر و یا حذف مشخصه‌های امنیتی کاربر (به عنوان مثال، تغییر کلمه عبور) مشاهده نماید.	
آزمون‌ها	
ارزیاب باید واسطه‌های مرتبط با مشخصه‌های امنیتی کاربر را بررسی و آزمون کند.	
۱۹	شناسایی کاربر ۱
محصول باید پیش از <u>شناسایی کاربر</u> اجازه اقدامات زیر را فراهم آورد:	
[انتخاب:	
- مشاوره راهنمای نحوه ورود به سیستم، [اختصاص: دیگر اقدامات]	
[	
اقدامات ارزیابی:	
خلاصه مشخصات محصول	
ارزیاب در «خلاصه مشخصات محصول» باید بررسی نماید که اطلاعات ارسالی در احراز هویت راه دور مشخص شده است.	
سند راهنمای محصول	
در راهنمای مدیریتی محصول، باید نحوه پیکربندی محصول برای ارتباط با کاربران راه دور توضیح داده شود.	
آزمون‌ها	
ارزیاب باید با استفاده از راهنمای محصول پیکربندی مناسبی برای احراز هویت تنظیم نماید. بنابراین در اعتبارسنجی/روش احراز هویت، باید نتایج اطلاعات مرتبط با احراز هویت صحیح جهت دسترسی به سیستم فراهم شود. در حالیکه، در منع دسترسی به سیستم، اطلاعات نادرست فراهم می‌شود.	
۲۰	شناسایی کاربر ۲

محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی مانند انجام عملیات برای فراموشی کلمه عبور و از این قبیل موارد وجود داشته باشد، با موفقیت شناسایی نماید.	
۲۱	احراز هویت کاربر ۱
محصول باید پیش از احراز هویت کاربر، اجازه اقدامات زیر را به کاربر دهد: [انتخاب:	
• مشاهده راهنمای نحوه ورود به سیستم، • شناسایی کاربر • [اختصاص: دیگر اقدامات]	
۲۲	احراز هویت کاربر ۲
محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، احراز هویت نماید.	
۲۳	سازوکار احراز هویت چندگانه ۱
محصول باید به منظور احراز هویت کاربر سازوکارهای زیر را فراهم آورد: [اختصاص:	
• نام کاربری و کلمه عبور • [انتخاب: امضای دیجیتال، یا هر متد احراز هویت جایگزین دیگر برای فراهم آوردن امنیت بهتر]	
انتخاب: سایر شیوه های احراز هویت امن طرف سوم دیگر مانند Active directory, OAuth2	

نکته کاربردی ۸:

برای احراز هویت کاربر باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد. به عنوان مثال، برای احراز هویت در محصول «نام کاربری و کلمه عبور، گواهی دیجیتال» استفاده می‌گردد.

اقدامات ارزیابی:

- خلاصه مشخصات محصول

ارزیاب باید در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی بررسی نماید که ساز و کار احراز هویت معرفی شده باشد.

- آزمون‌ها

برای آزمون این الزام، ابتدا باید الزام شماره‌ی ۲۱ «احراز هویت کاربر ۱» به طور کامل مورد تأیید قرار گرفته باشد. سپس ارزیاب باید همه ساز و کارهای احراز هویت قابل دسترس را پیکربندی نموده و واسطه‌های پشتیبان تمام ساز و کارهای احراز هویت را بررسی نماید.

۲۴ سازوکار احراز هویت چندگانه ۲

محصول باید هر کاربر متقاضی احراز هویت را مطابق [اختصاص: کاربران از راه دور باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احراز هویت چندگانه (مانند Dual factor authentication) استفاده کند، [اختصاص: OTP یا توکن و از این قبیل موارد] احراز هویت نماید.

اقدامات ارزیابی:

این الزام وابسته به الزام شماره ۲۳ «سازوکار احراز هویت چندگانه ۱» وابسته است.

۲۵ انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱

محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید:
[اختصاص:

- شناسه کاربر
- نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه
- جزئیات واسطه کلاینت
- پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)

- [اختصاص: لیست دیگر مشخصه‌های کاربری]

[

نکته کاربردی :

در اختصاص دوم می‌توان مواردی از قبیل آخرین دسترسی‌ها به موجودیت‌های غیرفعال را در نظر گرفت.

اقدامات ارزیابی:

- خلاصه مشخصات محصول

ارزیاب باید مشخصه‌های امنیتی کاربر که در بخش «خلاصه مشخصات ارزیابی» از سند هدف امنیتی آمده است را با مشخصاتی که در واسط محصول وجود دارد مطابقت دهد تا نسبت به پشتیبانی این الزام اطمینان حاصل نماید.

- سند راهنمای محصول

ارزیاب باید بخش راهنمای مدیریتی از سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید که نحوه ایجاد موجودیت فعال و امکان تغییر مشخصه‌های امنیتی آن بیان شده باشد.

- آزمون‌ها

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بتواند براساس سند راهنمای محصول، مشخصه‌های امنیتی را برای اجرای عملیات مقداردهی و ویرایش نماید. سپس چگونگی اعمال این تغییرات (موفقیت آمیز یا عدم موفقیت) را بررسی نماید. در برخی موارد این آزمون را باید همراه با کنترل دسترسی، محدودیت‌های مدیریتی امنیتی و یا در ممیزی صورت گیرد.

آزمون دوم: ارزیاب باید بتواند مشخصه‌های امنیتی را با توجه به راهنمای شرح محصول، با تمامی حداقل شرایط، مقداردهی و یا ویرایش نماید. همچنین ارزیاب با دریافت خطا هنگام بررسی و اعمال مقادیر مختلف در مشخصه‌های امنیتی می‌تواند متوجه شود که تغییرات مشخصه‌های امنیتی بدرستی اعمال نشده است. در برخی موارد باید این آزمون همراه با کنترل دسترسی، محدودیت‌های مدیریتی امنیتی و یا در ممیزی بررسی شود.

۲۶ انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲

محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید:

[اختصاص:

- زمانی که یک نشست جدید برقرار می‌شود، اعتبار نشست‌های قبلی باید از بین برود (به جزء مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد و هنگام فعال شدن نشست دوم و بیشتر در برنامه، باید به صفحه کاربر نشست اصلی(اول) اطلاع داده شود).
- اطلاعات پیشینه احراز هویت باید بروزرسانی گردد
- [اختصاص: دیگر قوانین برای اتصال اولیه مشخصه‌ها]

[

اقدامات ارزیابی

- **سند راهنمای محصول**

ارزیاب باید در سند راهنمای محصول توضیحاتی در خصوص نحوه‌ی ایجاد موجودیت‌های فعال و اعمال تغییر در مشخصه‌های امنیتی مرتبط با موجودیت‌های فعال مشاهده نماید.

- **آزمون‌ها**

ارزیاب ابتدا نشستی را با محصول آغاز نماید، و بعد از محصول خارج شود، ممکن است اطلاعات نشست به درستی منقضی نشده باشد لذا لازم است ارزیاب مجدد به سیستم ورود نماید و بررسی نماید که از شناسه نشست قبلی استفاده شده است یا خیر.

۲۷ | انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳

محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید:

[اختصاص: هیچ تغییری در طول نشست فعال مجاز نمی‌باشد، [اختصاص: دیگر قوانین حاکم بر تغییرات مشخصه‌ها]]

نکته کاربردی ۹:

منظور از تغییرات، به این معناست که هیچ یک از مشخصه‌های امنیتی کاربر تعریف شده در الزام شماره ۲۵ «انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱» در طول نشست تغییر نکند. تغییر نقش کاربر نیاز به لاگین مجدد دارد.

اقدامات ارزیابی

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب ابتدا با یک نام کاربری مشخص نشست را با محصول آغاز نماید، سپس یکی از مشخصه های امنیتی کاربر مانند آدرس IP سیستم را تغییر دهد در این صورت باید نشست غیرفعال و خاتمه یابد.

آزمون دوم: ارزیاب ابتدا نشست را با محصول با یک نام کاربری مشخص آغاز نماید، سپس اطلاعات نشست را به سیستم دیگر انتقال داده و تلاش نماید با همان اطلاعات نشست اتصال با محصول ادامه داشته باشد. در این حالت به دلیل تغییر سیستم و و تغییر محیط ارتباطی (با استفاده از مکانیزم های http only و یا دیگر توکن های تصادفی در کنار نشست که همچنین برای جلوگیری از CSRF نیز است می توان استفاده کرد) سیستم کاربر باید نشست خاتمه یابد و مجددا احراز هویت صورت گیرد.

آزمون سوم: ارزیاب ابتدا از طریق نام کاربری و مرورگر مشخص یک نشست با محصول آغاز نماید، سپس با مرورگر دیگری همان اطلاعات نشست را وارد نموده و تلاش نماید اتصال با محصول با همان اطلاعات نشست ادامه داشته باشد. در این صورت باید نشست خاتمه یابد و مجددا احراز هویت صورت گیرد.

۶,۴ کلاس حفاظت از داده های کاربری

شماره الزام	نام الزام
۲۸	حفاظت کامل از اطلاعات باقیمانده در منابع ۱

شماره الزام	نام الزام
	محصول باید تضمین نماید در هنگام [انتخاب: تخصیص منابع به، آزادسازی منابع از] تمام موجودیت های غیرفعال استفاده شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل دسترس می گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد. اقدامات تضمینی: • راهنما در صورت امکان پذیری پیکربندی و مدیریت کارکردهای منابع در محصول، انتظار می رود که توضیحاتی در خصوص نحوه ی پیکربندی مدیریت منابع و استفاده مجدد از آنها در سند راهنمای محصول بخش راهنمای مدیریتی محصول ارائه شده باشد. • آزمون ها ارزیاب باید تمام واسطه های که از منابع استفاده می کنند، بررسی نماید؛ همچنین قابل دسترس بودن اطلاعات قبلی را در هنگام استفاده مجدد منابع، توسط موجودیت فعال دیگر (یک کاربر دیگر) تجزیه و تحلیل نماید.
۲۹	ورود داده های کاربری به محصول با مشخصه امنیتی ۱ محصول باید هنگام دریافت داده کاربری، [اختصاص: خط مشی کنترل دسترسی] را اعمال نماید. اقدامات ارزیابی: • سند راهنمای محصول ارزیاب باید در سند راهنمای محصول توضیحاتی در خصوص نحوه ی کنترل و همچنین ورود داده کاربری ارائه نماید. • آزمون ها ارزیاب باید با توجه به پیکربندی و کنترل دسترسی که در راهنمای مدیریتی محصول آمده است، کاربری با مجوز ورود داده به داخل سیستم ایجاد نماید، و انجام درست عملیات را بررسی و تأیید نماید؛ همچنین با کاربری بدون مجوز وارد کردن داده، درستی یا عدم صحت عملیات بررسی گردد.
۳۰	ورود داده های کاربری به محصول با مشخصه امنیتی ۲

شماره الزام	نام الزام
	محصول باید از مشخصه‌های امنیتی مرتبط با داده‌های کاربری هنگام وارد کردن داده استفاده نماید. مشخصات امنیتی شامل مواردی از این قبیل است: نوع داده، حجم و اندازه فایل، فرمت فایل، تعداد دفعات Import کردن و از این قبیل موارد. نکته کاربردی ۱۰: مشخصه‌های امنیتی داده‌های کاربری می‌تواند شامل نوع داده، حجم داده، فرمت فایل و غیره باشد. اقدامات ارزیابی آزمون‌ها این آزمون وابسته به الزام شماره‌ی ۲۹ «ورود داده‌های کاربری به محصول با مشخصه امنیتی ۱» است. همچنین ارزیاب هنگام ورود داده به سیستم باید اطمینان حاصل نماید که تمامی مشخصه‌های امنیتی کاربر ذکر شده در راهنما همچون نام کاربری و یا امضاء دیجیتال و غیره نیز در نظر گرفته می‌شود. این بررسی در عملیاتی مانند «ثبت رکورد ممیزی عملیات ورود» با مشخصه امنیتی کاربر و همچنین «ذخیره داده وارده» با مشخصه امنیتی داده باید بررسی و تأیید شود.
۳۱	ورود داده‌های کاربری به محصول با مشخصه امنیتی ۳ محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال داده، ارتباط و همبستگی شفافیتی بین مشخصه‌های امنیتی و داده کاربری دریافت شده را فراهم می‌نماید و داده کاربر همانگونه که ادعا شده است (مبنی بر حفظ مسائل امنیتی) در برابر اطلاعات انتقال می‌یابد. اقدامات ارزیابی آزمون‌ها ارزیاب باید اطمینان حاصل نماید ورود داده به داخل محصول، مطابق پروتکل ادعا شده در سند راهنمای محصول صورت می‌گیرد و در هنگام انتقال شنود و گم شدن داده وجود ندارد.
۳۲	ورود داده‌های کاربری به محصول با مشخصه امنیتی ۴

شماره الزام	نام الزام
	محصول باید اطمینان دهد که تفسیر مشخصه‌های امنیتی داده‌های کاربری دریافت شده همانند، آنچه که فرستنده داده کاربری در نظر گرفته است، می‌باشد. اقدامات ارزیابی: آزمون‌ها ارزیاب باید داده‌ای را مطابق با آنچه که در سند راهنما محصول ذکر شده است به محصول ارسال نموده و بررسی نماید که تمام اطلاعات و داده‌ها به طور صحیح و کامل انتقال داده شده است.
۳۳	ورود داده های کاربری به محصول با مشخصه امنیتی ۵ محصول باید هنگام ورود داده کاربری از بیرون (خارج از محصول)، قوانین تحت کنترل خط‌مشی امنیتی زیر را اعمال نماید: [اختصاص: قوانین کنترلی اضافی هنگام ورود داده کاربری.] نکته کاربردی ۱۱: هدف الزامات مربوط به «ورود داده های کاربری به محصول»، ارائه کارکردهایی به منظور بررسی و صحت داده ورودی می‌باشد. به عنوان مثال، محصول برای کنترل داده‌های ورودی از سازوکاری همچون امضاء دیجیتال به منظور بررسی صحت استفاده نماید یا از مشخصه‌های امنیتی رکوردهای الکترونیکی، همچون خصیصه نوشتنی، خواندنی و غیره محافظت نماید. اقدامات ارزیابی: این الزام وابسته به الزام شماره ۲۹ «ورود داده های کاربری به محصول با مشخصه امنیتی ۱» و الزام شماره ۳۰ «ورود داده های کاربری به محصول با مشخصه امنیتی ۲» می‌باشد.
۳۴	خروج داده های کاربری از محصول با مشخصه امنیتی ۱

شماره الزام	نام الزام
	محصول باید هنگام خروج داده کاربری به بیرون ^۳ [اختصاص: خط‌مشی کنترل دسترسی] را اعمال نماید. اقدامات ارزیابی: • آزمون‌ها ارزیاب باید با توجه به پیکربندی و کنترل دسترسی که در سند راهنمای محصول محصول آمده است، «کاربری دارای مجوز خروج داده از داخل سیستم» ایجاد نموده و صحت انجام عملیات را بررسی نماید؛ سپس چگونگی انجام عملیات را بار دیگر با «کاربری بدون مجوز خروج داده از سیستم» بررسی نماید.
۳۵	خروج داده های کاربری از محصول با مشخصه امنیتی ۲
	محصول باید به همراه داده کاربری خروجی (انتقال داده به بیرون از محصول)، مشخصه‌های امنیتی مرتبط با داده کاربری را نیز انتقال دهد. اقدامات ارزیابی: • آزمون‌ها این آزمون وابسته به الزام شماره‌ی ۲۹ «ورود داده های کاربری به محصول با مشخصه امنیتی ۱» می‌باشد. ارزیاب هنگام خروج داده از سیستم باید اطمینان حاصل کند که مشخصه‌های امنیتی کاربر همانند نام کاربری و یا امضاء دیجیتال و غیره نیز در نظر گرفته می‌شود. همچنین باید بررسی گردد برای عملیات خروج با مشخصه امنیتی کاربر، رکورد ممیزی ثبت می‌گردد.
۳۶	خروج داده های کاربری از محصول با مشخصه امنیتی ۳
	محصول باید اطمینان دهد که مشخصه‌های امنیتی در هنگام خروج داده از محصول، ارتباط و پیوند شفاف با داده کاربری خارج شده دارند. اقدامات ارزیابی:

^۳ Export user data

شماره الزام	نام الزام
• آزمون ها این الزام وابسته به الزام شماره ی ۲۹ «ورود داده های کاربری به محصول با مشخصه امنیتی ۱» می باشد.	
۳۷	خروج داده های کاربری از محصول با مشخصه امنیتی ۴
محصول باید هنگام خروج داده کاربری به بیرون (خارج از محصول)، قوانین زیر را اعمال نماید: [اختصاص: مدیر سیستم باید خروج رکوردها را محدود نماید، به طوری که کاربران محصول بدون هدف قادر به خروج داده به بیرون از آن (خارج از محصول) نباشند.] اقدامات ارزیابی: • آزمون ها این الزام وابسته به الزام شماره ی ۲۹ «ورود داده های کاربری به محصول با مشخصه امنیتی ۱» می باشد.	
۳۸	صحت داده های کاربری ذخیره شده ۲
محصول باید داده کاربری حساس و یا دارای بار حقوقی ذخیره شده در مکان تحت کنترل خود را برای تشخیص [اختصاص: خطاهای صحت داده] داده های رکورد و داده های ممیزی را بر اساس مشخصه های [اختصاص: درهم شده^۴ داده های کاربری ذخیره شده] پایش نماید. اقدامات ارزیابی: • خلاصه مشخصات محصول در این فصل از سند هدف امنیتی باید در مورد پیاده سازی تشخیص خطای صحت توضیحاتی بیان شده باشد.	

^۴ Hash

شماره الزام	نام الزام
۳۹	صحت داده های کاربری ذخیره شده ۳
هنگام تشخیص خطای صحت داده، محصول باید [اختصاص: اقدام لازم] را صورت دهد. نکته کاربردی ۱۲: مشخصه های داده کاربری می تواند انواع فایل ها، اندازه فایل و محتوای فایل باشد. محصول به منظور شناسایی خطای صحت داده ها باید مشخصه های داده های کاربری را مانیتور کند تا در صورت تغییر و یا حذف، هشدار دهد. می توان برای تشخیص صحت داده ها از روش هایی همچون HMAC و یا ECC Checksum و دیگر روش های درهم سازی استفاده نمود.	
۴۰	خط مشی کنترل دسترسی ۱
محصول باید [اختصاص: خط مشی های کنترل دسترسی] را بر روی موارد زیر اعمال نماید: [اختصاص: • موجودیت فعال: [اختصاص: مدیر سیستم، کاربر عادی، [اختصاص: دیگر موجودیت های فعال]] • موجودیت غیر فعال: ○ رکوردها، مستندات ○ داده های متعلق به کاربر ○ داده احراز هویت ○ داده با این معیارها: [اختصاص: معیارهای داده] ○ [اختصاص: دیگر موجودیت های غیر فعال که شامل خط مش کنترل دسترسی می باشند] • عملیات: ○ ایجاد موجودیت غیر فعال جدید	

شماره الزام	نام الزام
○	حذف موجودیت غیرفعال
○	تغییر دسترسی‌ها به موجودیت غیرفعال
○	عملیات بر روی فراداده‌های وابسته به موجودیت غیرفعال
○	[اختصاص: دیگر عملیات‌ها]
[	
اقدامات ارزیابی	
• خلاصه مشخصات محصول در این فصل از سند هدف امنیتی، باید سازوکار کنترل دسترسی محصول و مشخصه‌های امنیتی مورد استفاده در خط‌مشی کنترل دسترسی به طور خلاصه توضیح داده شود. • سند راهنمای محصول ارزیاب باید سند راهنمای محصول را بررسی نموده و تأیید نماید توضیحاتی در خصوص خط‌مشی کنترل دسترسی و قوانین کنترل دسترسی برای مدیریت مشخصه‌های امنیتی ارائه شده است. همچنین ارزیاب باید این سند را در خصوص بیان چگونگی پیکربندی خط‌مشی کنترل دسترسی شامل مقداردی پیش فرض مشخصه‌های امنیتی و انتساب مجوزهای مورد نیاز برای عملیات مدیریتی بررسی نماید. • آزمون‌ها ارزیاب باید برای این الزام موارد زیر را بررسی نماید: ✓ تمام الگوریتم‌های کنترل دسترسی ذکر شده در سند هدف امنیتی ✓ برای هر الگوریتم کنترل دسترسی تمام شرایط ذکر شده در سند هدف امنیتی باید سنجیده شود (مانند شرایط منتهی شده به "yes" یا "no") ✓ مجموعه ترکیباتی از تنظیمات مشخصه‌های امنیتی مورد استفاده در الگوریتم‌های کنترل دسترسی همچنین باید برای این الزام کارکردهای مدیریتی مورد استفاده برای مدیریت مشخصه‌های امنیتی (مشخصه‌های امنیتی که در الگوریتم کنترل دسترسی استفاده می‌شوند) آزمون و بررسی شوند.	

شماره الزام	نام الزام
۴۱	عملیات کنترل دسترسی ۱
محصول باید [اختصاص: خط مشی های کنترل دسترسی] را با توجه به موارد زیر بر روی موجودیت های غیرفعال اعمال نماید: [اختصاص: • هویت کاربر • نقش ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می شوند • [اختصاص: دیگر مشخصه های موجودیت فعال]] اقدامات ارزیابی: الزامات عملیات کنترل دسترسی به الزام شماره ی ۴۰ «خط مشی کنترل دسترسی ۱» وابسته می باشد و همراه با آن الزام بررسی می شوند.	
۴۲	عملیات کنترل دسترسی ۲
محصول باید قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نمایند: [اختصاص: عملیات تنها به شرطی مجاز است که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد.]	
۴۳	عملیات کنترل دسترسی ۳

شماره الزام	نام الزام
	محصول باید براساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: [اختصاص: • کاربران با مجوز مدیر سیستم به رکوردهای لازمه مدیریت سیستم و نیز روش ارائه شده توسط محصول، دسترسی دارند. • کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند. • [اختصاص: دیگر قوانین] [
۴۴	عملیات کنترل دسترسی ۴
	محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید: [اختصاص: • تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه^۵ از پیش تعریف شده، • [اختصاص: دیگر قوانین] [اقدامات ارزیابی: وابسته به الزام شماره ی ۴۳ «عملیات کنترل دسترسی ۳» می باشد.

^۵ Threshold

۶,۵ کلاس مدیریت امنیت

شماره الزام	نام الزام
۴۵	مدیریت کارکرد در محصول ۱
محصول باید امکان [انتخاب: تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] کارکرد [اختصاص: تمام کارکردهای مربوط به مدیریت محصول] را به [اختصاص: مدیر سیستم و هر کاربری که مجوز لازم را دارد، [اختصاص: دیگر نقش ها]] محدود نماید. نکته کاربردی ۱۳: مثالی از این اختصاص: محصول باید امکان «تغییر رفتار» کارکرد جمع آوری داده های سیستم، آنالیز و عکس العمل را تنها به مدیران مجاز سیستم محدود نمایند. اقدامات ارزیابی: • خلاصه مشخصات محصول • ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی، هریک از کارکرد مدیریتی معرفی شده در راهنما (که از طریق واسط قابل دسترسی هستند) را بررسی و تأیید کند. • سند راهنمای محصول ارزیاب باید لیست کارکردهای محصول را در این سند بررسی و تأیید نماید و همچنین ذکر چگونگی پیکربندی و تنظیمات کارکردها در محصول را بررسی نماید.	

شماره الزام	نام الزام
• آزمون‌ها ارزیاب باید یکبار با مجوز مدیر سیستم سعی در تغییر پیکربندی کارکردهای محصول مطابق با سند راهنمای محصول نماید و بار دیگر با حساب کاربری غیرمجاز تلاش به غیرفعال نمودن و یا تغییر تنظیمات اعمال شده در کارکردها نماید.	
۴۶	مدیریت مشخصه‌های امنیتی ۱
محصول باید با اعمال [اختصاص: خط‌مشی کنترل دسترسی]، امکان [انتخاب: تغییر پیش‌فرض، پرس و جو، تغییر، حذف، [اختصاص: دیگر عملیات‌ها]] مشخصه‌های امنیتی [اختصاص: لیستی از مشخصه‌های امنیتی تعریف شده در الزام انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱] را به [مدیر سیستم و هر کاربری که مجوز لازم را دارد [اختصاص: دیگر نقش‌ها]] محدود نماید. اقدامات ارزیابی: • سند راهنمای محصول ارزیاب باید سند راهنمای محصول را بررسی نماید و اطمینان حاصل نماید در خصوص شرایطی که یک کاربر اجازه مدیریت مشخصه‌های امنیتی موجودیت‌های غیرفعال را دارد توضیحاتی ارائه شده است. • آزمون‌ها ارزیاب باید تمامی واسط‌های مرتبط با مدیریت مشخصه‌های امنیتی موجودیت‌های غیرفعال و تمام مشخصه‌های امنیتی موجودیت‌های غیرفعال با مقداردی آن‌ها (البته به عنوان بخشی از آزمون الگوریتم کنترل دسترسی در الزام قبل بررسی می‌شوند) را آزمون نماید.	
۴۷	مقدار دهی اولیه مشخصه‌ها ۱
محصول برای مشخصه‌های امنیتی که برای اعمال [اختصاص: خط‌مشی] استفاده می‌شوند، باید مقادیر پیش فرض [انتخاب: محدود شده‌ای]، در نظر بگیرد.	

شماره الزام	نام الزام
اقدامات ارزیابی: به الزام شماره ۴۵ «مدیریت کارکرد در محصول ۱» وابسته است.	
۴۸	مقدار دهی اولیه مشخصه‌ها ۲
محصول برای تعیین مقادیر اولیه پیشنهادی باید به [اختصاص: مدیر سیستم و هر کاربری که مجوز لازم را دارد] اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش فرض را لغو و تغییر دهد.	
۴۹	مدیریت داده های محصول ۱-مدیر سیستم
محصول باید امکان [انتخاب: تغییر پیش فرض، پرس و جو، تغییر، حذف، پاک نمودن، [اختصاص: دیگر کارکردها]] [اختصاص: لیستی از داده‌های محصول] به [اختصاص: مدیر سیستم و هر کاربری که مجوز لازم را دارد [اختصاص: دیگر نقش‌ها]] محدود نماید.	
نکته کاربردی ۱۴: داده‌های محصول می‌تواند شامل داده‌های ممیزی، کلیدها و داده‌های احراز هویت و از این نوع داده‌ها باشد. مثالی از این الزام: محصول امکان مدیریت داده‌های خود را تنها به مدیر امنیتی محدود می‌نماید. «مدیریت» در این الزام می‌تواند شامل موارد زیر باشد: ایجاد، مقداردهی، مشاهده، تغییر پیش فرض، تغییر دادن، حذف نمودن، پاک کردن و اضافه نمودن اقدامات ارزیابی: به الزام شماره ۴۵ «مدیریت کارکرد در محصول ۱» وابسته است.	
۵۰	مدیریت داده های محصول ۱-کاربر عادی، وارد کننده داده

شماره الزام	نام الزام
محصول باید امکان [انتخاب: تغییر پیش فرض، پرس و جو، تغییر، حذف، پاک نمودن، [اختصاص: دیگر کارکردها]] [اختصاص: داده‌های تحت مالکیت کاربر عادی] را به [اختصاص: کاربر عادی] محدود نماید. اقدامات ارزیابی: به الزام شماره ۴۵ «مدیریت کارکرد در محصول ۱» وابسته است. همچنین ارزیاب باید حداقل یکی از کارکردهای محصول در این الزام را با کاربری غیرمجاز آزمون نماید.	
۵۱	کارکردهای مدیریتی محصول ۱
محصول باید قادر به انجام [اختصاص: کارکردهای مدیریتی که در جدول زیر آمده است] باشد:	
مؤلفه	عملیات مدیریتی
بازبینی داده ممیزی ۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی ۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۱	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
عملیات کنترل دسترسی	مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع
حفاظت کامل از اطلاعات باقیمانده در منابع	انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزاد سازی) که می‌تواند در محصول قابل پیکربندی باشد.
ورود داده‌های کاربری به محصول با مشخصه امنیتی	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
صحت داده‌های کاربری ذخیره شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد.

شماره الزام	نام الزام
مدیریت احراز هویت ناموفق	مدیریت حد آستانه برای تلاش های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احراز هویت باید صورت گیرد.
تعریف مشخصات کاربر	مدیر مجاز باید قادر به تعریف مشخصه های امنیتی بیشتر برای کاربران باشد. [اختیاری]
مدیریت کلمه عبور	مدیریت تنظیمات و الزامات و قابلیت ها برای تنظیم کلمه عبورها
احراز هویت کاربر	مدیریت داده های احراز هویت توسط مدیر یا کاربر مرتبط مدیریت یکسری عملیاتی که قبل از احراز هویت کاربر انجام می شوند.
سازوکار احراز هویت چندگانه	مدیریت سازوکارهای احراز هویت مدیریت قوانین مرتبط با احراز هویت
شناسایی کاربر	مدیریت شناسایی کاربران [اختیاری] مدیریت تغییرات و فرایندهایی مانند (اختصاص ادرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می تواند قبل از شناسایی کاربر انجام دهد.
انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	مدیر مجاز می تواند مشخصه های امنیتی موجودیت های فعال پیش فرض را تعریف و تغییر دهد.
مدیریت مشخصه های امنیتی	مدیریت گروهی از نقش هایی که با مشخصه های امنیتی در تعامل هستند.
مقدار دهی اولیه مشخصه ها	مدیریت گروهی از نقش هایی که مقادیر اولیه را مشخص می کنند. مدیریت مقادیر پیش فرض برای کنترل دسترسی محصول
مدیریت داده های محصول ۱-مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده های محصول
مدیریت داده های محصول ۱-کاربر عادی، وارد کننده داده	مدیریت گروهی از قوانینی مرتبط با داده های محصول
نقش های امنیتی	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
محدودیت بر روی چندین نشست همزمان	مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر
برقراری نشست	مدیریت شرایط آغاز نشست توسط مدیر مجاز
خاتمه دادن به نشست ها	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد.

شماره الزام	نام الزام
	تعیین زمان پیش فرض غیرفعال بودن کاربر که نشست خاتمه یابد.
اقدامات ارزیابی: • خلاصه مشخصات محصول تمام کارکردهای امنیتی محصول به طور خلاصه باید در این بخش توضیح داده شود.	
۵۲	نقش های امنیتی ۱
نقش های زیر در محصول باید تعریف شده باشد: [انتخاب: مدیر سیستم، کاربر عادی، [اختصاص: دیگر نقش های مجاز معرفی شده]]	
نکته کاربردی ۱۵: از جمله نقش های مجاز می توان به «مدیر مجاز»، «مدیر تحلیلگر مجاز»، «اپراتورها» اشاره نمود، نویسنده سند هدف امنیتی در این الزام می تواند از نقش های مجاز دیگر نیز استفاده نماید.	
اقدامات ارزیابی: • خلاصه مشخصات محصول ارزیاب باید در این فصل از سند هدف امنیتی بررسی و تأیید نماید توضیحاتی در خصوص نقش مدیریتی و نقش هایی با دسترسی پایین ارائه شده است.	
• سند راهنمای محصول	

شماره الزام	نام الزام
	ارزیاب باید بخش راهنمای مدیریتی از سند راهنمای محصول را بررسی نموده و در خصوص ارائه دستورالعمل هایی برای مدیریت محصول هم به طور محلی و از راه دور و همچنین پیکربندی هایی مورد نیاز برای مدیریت راه دور اطمینان حاصل نماید. • آزمون ها ارزیاب باید اطمینان حاصل نماید که نقش مدیریتی می تواند تمامی کارکردهای امنیتی محصول که در سند هدف امنیتی ذکر شده است را مدیریت نماید. ارزیاب باید نقش مدیریتی و یا کاربر با یک نقش محدود را به طور محلی و یا از راه دور بر روی محصول آزمون نماید.
۵۳	نقش های امنیتی ۲
	محصول، باید قادر به مرتبط نمودن کاربران با نقش ها و دسترسی های مجاز تعریف شده باشند. نکته کاربردی ۱۶: لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد. اما ممکن است نقش ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند. اقدامات ارزیابی: این الزام وابسته به الزام شماره ی ۵۲ «نقش های امنیتی ۱» می باشد.

۶,۶ کلاس حفاظت از توابع امنیتی محصول

شماره الزام	عنصر امنیتی
۵۴	حفظ وضعیت امن در زمان شکست ۱
محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: [اختصاص: شکست‌های نرم‌افزاری، شکست‌های کاربری] نکته کاربردی ۱۷: شکست نرم‌افزاری به معنی از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول می‌باشد که در این صورت محصول باید در وضعیت امنی قرار گرفته و صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید. اقدامات ارزیابی: • خلاصه مشخصات محصول ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی، بررسی نماید توضیحاتی در خصوص پیاده‌سازی شکست امن محصول، انواع مدهای شکست محصول و وضعیت امن هر کدام از شکست‌ها نیز ارائه شده باشد. • آزمون‌ها ارزیاب باید انواع شکست‌ها را ایجاد و با وضعیت امن مقایسه و بررسی نماید.	
۵۵	سازگاری داده‌های امنیتی بین محصول و موجودیت امن ۱
محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار [اختصاص: لیستی از انواع داده‌های امنیتی محصول] را در زمان اشتراک‌گذاری داده‌های امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد. نکته کاربردی ۱۸: منظور از داده‌های امنیتی محصول، داده‌های احراز هویت، کلید، امضای دیجیتال، داده‌های ممیزی و از این نوع داده‌ها است.	

شماره الزام	عنصر امنیتی
اقدامات ارزیابی: • سند راهنمای محصول در بخش راهنمای مدیریتی از سند راهنمای محصول باید توضیحاتی در خصوص انواع داده های امنیتی محصول و داده های دریافتی از دیگر محصولات امن IT ارائه شده باشد.	
۵۶	سازگاری داده های امنیتی بین محصول و موجودیت امن ۲
محصول باید هنگام تفسیر داده های دریافتی از دیگر محصولات IT امن، [اختصاص: لیستی از قوانین تفسیر که در محصول به کار می روند] را استفاده نماید. اقدامات ارزیابی: • آزمون ها ارزیاب باید با بررسی داده های دریافتی از دیگر محصولات در داخل محصول نسبت به انطباق داده های محصول با آنچه که ادعای محصول است، اطمینان حاصل نماید.	
۵۷	انتقال داده امنیتی در داخل محصول ۱
محصول باید توانایی داشته باشد که در صورت فراهم نمودن بستر و زیرساخت امن، از افشاء یا تغییر داده ها در هنگام انتقال بین بخش های مجزای خود که باهم ارتباط دارند، محافظت نماید. نکته کاربردی ۱۹:	

شماره الزام	عنصر امنیتی
	منظور از بخش‌های مجزا به این معنی است که بخش‌های محصول بر روی دو سیستم مجزا قرار گرفته باشد، مانند وب سرور بر روی یک سیستم و بانک اطلاعاتی روی سیستم دیگر در یک شبکه عمومی باشد و یا دو بخش مجزای محصول یکی بر روی وب سرور و دیگری بر روی کلاینت باشد. اقدامات ارزیابی: • خلاصه مشخصات محصول ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی بررسی نماید در خصوص روش یا پروتکل‌های استفاده شده برای انتقال داده بین اجزای توزیع‌شده محصول توضیحاتی ارائه شده است. • سند راهنمای محصول ارزیاب باید با بررسی سند راهنمای محصول، نسبت به ارائه توضیحاتی در خصوص روش یا پروتکل ارتباطی بین اجزای محصول اطمینان حاصل نماید. • آزمون‌ها ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید روش ارتباطی ذکر شده در سند راهنمای محصول را آزمون نماید. آزمون دوم: ارزیاب باید اطمینان حاصل نماید که داده‌ها بین اجزای محصول بصورت آشکار نمایش داده نشود. آزمون سوم: ارزیاب باید اطمینان حاصل نماید که ویرایش داده‌ها حین انتقال، توسط محصول تشخیص داده شود.
۵۸	مهرهای زمانی ۱
	محصول، باید قادر به ایجاد مهرهای زمانی قابل اطمینان باشند و یا این نیازمندی را از طریق سرورهای امن و مکانیزم کارکردی صحیح برطرف نماید.

شماره الزام	عنصر امنیتی
اقدامات ارزیابی: خلاصه مشخصات محصول ارزیاب باید اطمینان حاصل نماید در فصل «خلاصه مشخصات محصول» از سند هدف امنیت هریک از کارکردهای امنیتی استفاده کننده از زمان لیست شده باشد. سند راهنمای محصول ارزیاب باید سند راهنمای محصول را بررسی نماید، تا در خصوص ارائه ی دستورالعمل هایی در مورد تنظیمات و پیکربندی زمان اطمینان حاصل نماید. آزمون ها ارزیاب باید اقدامات زیر را اجرا کند: آزمون اول: ارزیاب باید مطابق سند راهنمای محصول، زمان را پیکربندی نموده و سپس با توجه به واسط مربوطه از صحت عملکرد آن اطمینان حاصل نماید. آزمون دوم: ارزیاب باید توسط کاربر نامجاز و با استفاده از واسط مربوطه، سعی در تغییر پیکربندی زمان نماید. آزمون سوم: اگر محصول از سرور NTP پشتیبانی می کند باید کلاینت NTP را بر روی محصول پیکربندی نموده و زمان سرور و کلاینت را بررسی نماید.	
۵۹	به روز رسانی امن ۲
محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کارشناس شرکت تولید کننده محصول فراهم نماید که به روزرسانی نرم افزار و میان افزار محصول مورد ارزیابی را به صورت دستی آغاز نماید و [انتخاب: از جستجوی خودکار به روزرسانی ها پشتیبانی کند، از به روزرسانی های خودکار پشتیبانی کند، از مکانیزم به روزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به روزرسانی، از هیچ مکانیزم به روزرسانی پشتیبانی نکند].	

شماره الزام	عنصر امنیتی
نکته کاربردی ۲۰: عبارت «انتخاب» در این الزام بین پشتیبانی از «جستجوی خودکار به روزرسانی ها» و «به روزرسانی خودکار» تمایز قائل می شود. جستجوی خودکار به روزرسانی ها به یک محصول مورد ارزیابی اشاره دارد که جستجو می کند تا ببیند به روزرسانی جدیدی وجود دارد یا خیر، و این امر را به مدیر سیستم اطلاع می دهد (مثلاً از طریق یک پیام یا یک پرچم)؛ اما نصب به روزرسانی نیازمند انجام اقداماتی توسط مدیر سیستم خواهد بود. اما به روزرسانی خودکار به یک محصول مورد ارزیابی اشاره دارد که به روزرسانی ها را جستجو می کند و در صورت وجود آن ها را نصب می نماید.	
۶۰	به روز رسانی امن ۳
محصول مورد ارزیابی باید در صورت استفاده از به روز رسانی به روش خودکار، پیش از نصب به روزرسانی های نرم افزاری و میان افزاری، با استفاده از [انتخاب: مکانیزم امضای دیجیتال، درهم ساز منتشر شده]، ابزاری را برای احراز هویت میان افزار آن ها در اختیار محصول مورد ارزیابی قرار دهد.	

۶,۷ کلاس دسترسی به محصول

شماره الزام	عنصر امنیتی
۶۱	محدودیت بر روی چندین نشست همزمان ۱
محصول باید حداکثر تعداد نشست های همزمان متعلق به یک کاربر را محدود نماید. نکته کاربردی ۲۱: محصول می تواند انتخاب عملیاتی را که بعد از پر شدن نشست های همزمان باید روی دهد را به مدیر سیستم و یا کاربر دارای مجوز بدهد.	

شماره الزام	عنصر امنیتی
اقدامات ارزیابی: • سند راهنمای محصول ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید توضیحاتی در خصوص نحوه‌ی پیکربندی تعداد نشست همزمان برای یک کاربر در راهنمای محصول ارائه شده است. • آزمون‌ها ارزیاب باید با توجه به سند راهنمای محصول حداکثر نشست یک کاربر را پیکربندی نماید و سپس با همان کاربر از چند سیستم به طور همزمان سعی در ایجاد نشست نماید. در این صورت اگر تعداد نشست بیش از مقدار مشخص شده باشد باید اجازه ایجاد نشست را ندهد.	
۶۲	محدودیت بر روی چندین نشست همزمان ۲
محصول باید به صورت پیش‌فرض، [اختصاص: تعداد نشست همزمان پیش‌فرض] برای هر کاربر در نظر بگیرد. اقدامات ارزیابی: وابسته به الزام شماره‌ی ۶۱ «محدودیت بر روی چندین نشست همزمان ۱» می‌باشد.	
۶۳	خاتمه دادن به نشست‌ها توسط محصول ۱
محصول باید کلیه نشست‌های تعاملی راه دور^۶ را پس از مدت زمان [اختصاص: بازه زمانی که توسط مدیر تنظیم می‌شود] غیرفعال بودن، خاتمه دهد. اقدامات ارزیابی:	

^۶Remote

شماره الزام	عنصر امنیتی
	• سند راهنمای محصول - در راهنمای محصول باید در خصوص نحوه‌ی پیکربندی زمان غیرفعال بودن نشست توضیحاتی بیان شده باشد. • آزمون‌ها - ارزیاب باید مطابق سند راهنمای محصول، مقادیر مختلف برای زمان غیرفعال بودن نشست تنظیم و پیکربندی نماید که این مقادیر شامل حداقل و حداکثر زمان غیرفعال بودن طبق سند راهنما باشند. سپس ارزیاب برای هر زمان تنظیم شده نشست از راه دور با محصول ایجاد و درستی زمان غیرفعال بودن نشست را بررسی نماید که باعث خاتمه یافتن نشست می‌شود.
۶۴	خاتمه دادن به نشست ها توسط کاربر ۱
	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد. اقدامات ارزیابی: • آزمون‌ها - ارزیاب باید اقدامات زیر را اجرا نماید: - آزمون اول: ارزیاب باید نشست محلی با محصول ایجاد نموده و سپس مطابق راهنما با استفاده از موارد "Exit" یا "Log out" از محصول خارج شود و بررسی نماید که آیا نشست خاتمه یافته است. - آزمون دوم: ارزیاب باید نشست از راه دور با محصول ایجاد نموده و سپس مطابق راهنما با استفاده از موارد "Exit" یا "Log out" از محصول خارج شود و بررسی نماید که آیا نشست خاتمه یافته است.
۶۵	سوابق دسترسی به محصول ۱
	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست براساس [انتخاب: روز، زمان،] اختصاص: دیگر مشخصه‌ها]] باشد.
۶۶	سوابق دسترسی به محصول ۲

شماره الزام	عنصر امنیتی
	در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست براساس [انتخاب: روز، زمان،] اختصاص: دیگر مشخصه ها]] و تعداد تلاش ناموفق تا آخرین ایجاد نشست موفقیت آمیز باشد. اقدامات ارزیابی • سند راهنمای محصول باید در این سند در خصوص نحوه ی پیکربندی نمایش تعداد و آخرین تلاش ناموفق توضیحاتی ارائه شده باشد. • آزمون ها ارزیاب چندین بار با استفاده از یک نام کاربری با شرایطی غیرمجاز (مانند کلمه عبور نادرست) تلاش به برقراری نشست با محصول نماید و سپس یک نشست موفقیت آمیزی را برقرار نماید و بررسی نماید که تعداد تلاش های ناموفق کاربر و زمان آخرین تلاش برای برقراری نشست در محصول ثبت شده باشد.
۶۷	سوابق دسترسی به محصول ۳ محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر از واسط کاربری پاک نماید. اقدامات ارزیابی • سند راهنمای محصول در صورت وجود امکان پیکربندی اطلاعات سوابق دسترسی، باید در بخش راهنمای مدیریتی از سند راهنمای محصول توضیحاتی ارائه شده باشد.
۶۸	برقراری نشست ۱ محصول باید قادر به ممانعت از ایجاد نشست براساس [انتخاب: مکان، شماره پورت، روز، زمان،] اختصاص: دیگر مشخصه ها]] باشد. اقدامات تضمینی: • خلاصه مشخصات محصول

شماره الزام	عنصر امنیتی
	ارزیاب باید با بررسی فصل «خلاصه مشخصات محصول» از سند هدف امنیتی نسبت به تعریف تمام مشخصه های کلاینتی که باید نشست آن منع شود، اطمینان حاصل نماید. • راهنما ارزیاب باید در سند راهنمای محصول، بررسی نماید توضیحاتی در خصوص پیکربندی هر مشخصه ای که در «خلاصه مشخصات محصول» آمده است (مشخصه هایی مانند آدرس IP، زمان/تاریخ، آدرس فیزیکی و ...) ارائه شده است. • آزمون ها ارزیاب باید برای هر یک از مشخصه ها، آزمون زیر را انجام دهد: آزمون اول: ارزیاب باید با یک کاربر یک نشست موفقیت آمیزی را ایجاد نماید، سپس مطابق راهنما، مشخصه های کاربر را به گونه ای پیکربندی نماید که از دسترسی آن کاربر به محصول ممانعت شود. ارزیاب باید تلاش در برقراری نشستی نماید که مشخصه ای از آن (مانند آدرس IP و یا مکان کاربر) برای دسترسی منع شده باشد و سپس عدم موفقیت کاربر در تلاش برای دسترسی را مشاهده نماید.

۶,۸ کلاس تخصیص منابع

شماره الزام	عنصر امنیتی
۶۹	تحمل خطا ۱
محصول باید از عملکرد [اختصاص: تمام کارکردهای اصلی] هنگام رویداد شکست های زیر اطمینان حاصل نماید: [اختصاص: شکست نرم افزاری، [اختصاص: انواع دیگر شکست ها]]	

شماره الزام	عنصر امنیتی
اقدامات ارزیابی: آزمون‌ها ارزیاب باید شکستی را ایجاد و سپس بررسی نماید که کارکردهای اصلی (مانند ممیزی) بدرستی کار می‌کنند یا خیر.	

۶,۹ کلاس کانال‌ها/مسیرهای مورد اعتماد

برای این کلاس، تعدادی الزام مبتنی بر انتخاب در «پیوست دو» ارائه شده است.

شماره الزام	نام الزام
۷۰	مسیر امن ۱
محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [انتخاب: TLS, HTTPS] مسیر ارتباطی امنی فراهم نماید تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه دور ایجاد شود که به طور منطقی از دیگر کانال‌ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده‌های تبادلی حفاظت نماید و تغییرات را تشخیص دهد. نکته کاربردی ۲۲: کاربر عمومی مجوز ورود به محصول را ندارد. نویسنده سند هدف امنیتی در صورت استفاده از TLS باید الزامات آن را از «پیوست دو» به سند هدف امنیتی اضافه نماید.	
۷۱	مسیر امن ۲
محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	
۷۲	مسیر امن ۳

شماره الزام	نام الزام
محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه دور مدیر سیستم الزامی نماید.	
نکته کاربردی ۲۳:	
این الزام اطمینان حاصل می‌نماید که مدیران سیستم معتبر، تمام ارتباطات از راه دور را با محصول مورد ارزیابی، از طریق یک مسیر امن آغاز می‌کنند و در طی ارتباط با محصول مورد ارزیابی، همچنان از مسیر امن استفاده می‌نمایند. داده‌های منتقل شده از طریق این مسیر، با استفاده از پروتکل انتخاب شده در عبارت انتخاب، رمزگذاری می‌شوند.	

۷ الزامات تضمین امنیت

اهداف امنیتی تعریف شده در بخش ۵ جهت مقابله نمودن با تهدیدات معرفی شده در بخش ۴ در نظر گرفته شده‌اند. الزامات کارکردی در بخش ۶ بیان رسمی و استاندارد از «اهداف امنیتی» می‌باشد. الزامات تضمین امنیتی که برگرفته از استاندارد ارزیابی امنیتی معیار مشترک می‌باشند تا براساس این الزامات ارزیابی، مستندات را ارزیابی و آزمون مستقل بر روی محصول انجام دهد.

مدل کلی ارزیابی محصول در برابر سند هدف امنیتی که مطابق این پروفایل حفاظتی است، به صورت زیر می‌باشد:

پس از تأیید سند هدف امنیتی برای ارزیابی، تولیدکننده محصول رادر اختیار آزمایشگاه قرار می‌دهد و محیط آزمون آن را فراهم می‌نماید. و سپس فعالیت‌های تضمین که در سند هدف امنیتی مطرح شده، توسط آزمایشگاه انجام می‌شود. نتایج این فعالیت‌ها مستند و برای اعتباربخشی به مرکز گواهی ارائه می‌شود.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی

آزمون مستقل-منطبق	ATE_IND.1	Tests
تحلیل آسیب پذیری	AVA_VAN.1	Vulnerability Assessment
برچسب گذاری محصول	ALC_CMC.1	Life cycle Support
پوشش پیکربندی محصول	ALC_CMS.1	

۷.۱ کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نمی باشد، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تأیید توسعه دهندگان محصول باشد.

مشخصات کارکردی:

مشخصات کارکردی، واسطه های کارکرد امنیتی محصول را توصیف می نماید اما نیازی به شرح مفصل و کاملی از این واسطه ها نمی باشد. فعالیت های این خانواده باید بر روی شناخت واسطه های معرفی شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
مشخصات کارکردی (ADV_FSP)	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.1D) شرح مؤلفه: توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.2D)

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
	شرح مؤلفه: توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. نکته کاربردی: مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
مشخصات کارکردی (ADV_FSP)	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.1C) شرح مؤلفه: مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی^۷ و پشتیبان کننده‌ی الزام کارکرد امنیتی^۸ توصیف نماید.

^۷-SFR-enforcing TSFI^۸-SFR-supporting TSFI

مؤلفه های محتوایی	
نام خانواده	عنصر امنیتی
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.2C) شرح مؤلفه: مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.3C) شرح مؤلفه: مشخصات کارکردی باید برای دسته بندی ضمنی واسط های غیر مداخله کننده ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.4C) شرح مؤلفه: ردیابی باید نشان دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
مشخصات کارکردی	نام عنصر: مشخصات کارکرد ابتدایی ۱

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
(ADV_FSP)	شماره مؤلفه: (ADV_FSP.1.1E) شرح مؤلفه: ارزیاب باید تأیید نماید که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مؤلفه: (ADV_FSP.1.2E) شرح مؤلفه: ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «آزمون» و «آسیب‌پذیری» ارائه شده است.

۷,۲ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود. برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل: دستورالعمل نصب موفقیت آمیز محصول در محیط دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر دستورالعمل‌هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو می‌باشد.

۷,۲,۱ راهنمای کاربردی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
راهنمای کاربردی (AGD_OPE)	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.1D) شرح مؤلفه: توسعه دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه های محتوایی	
نام خانواده	عنصر امنیتی
راهنمای کاربردی (AGD_OPE)	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.1C) شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.2C) شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسطه های در دسترس ارائه شده توسط محصول به صورت امن استفاده می گردد.
	نام عنصر: راهنمای کاربردی ۱

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	شماره مؤلفه: (AGD_OPE.1.3C) شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسطه‌های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.4C) شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت-های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.5C) شرح مؤلفه: سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.6C) شرح مؤلفه:

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.7C) شرح مؤلفه: سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
راهنمای کاربردی (AGD_OPE)	نام عنصر: راهنمای کاربردی ۱ شماره مؤلفه: (AGD_OPE.1.1E) شرح مؤلفه: ارزیاب باید تأیید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۷,۲,۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
راهنمای آماده‌سازی (AGD_PRE)	نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.1D) شرح مؤلفه: توسعه دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
راهنمای آماده‌سازی (AGD_PRE)	نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.1C) شرح مؤلفه: مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.2C) شرح مؤلفه: مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مؤلفه‌های اقدامات ارزیاب	
راهنمای آماده‌سازی (AGD_PRE) نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.1E) شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	
نام عنصر: راهنمای آماده‌سازی ۱ شماره مؤلفه: (AGD_PRE.1.2E) شرح مؤلفه: ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به صورت امن برای عمل نمودن آماده شود.	

۷.۳ کلاس آزمون

آزمون محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آنها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. آزمون بخش‌های کارکردی سیستم از طریق خانواده ATE_IND؛ و آزمون بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون براساس کارکردی که برای محصول در نظر گرفته شده و واسطه‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج آزمون و تحلیل آسیب‌پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

۷,۳,۱ آزمون مستقل

«آزمون مستقل» برای تأیید کارکرد محصول که در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و مستندات «راهنمای مدیر» ارائه شده، صورت می گیرند. هدف اصلی آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می باشد. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند نماید.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
آزمون مستقل (ATE_IND)	نام عنصر: آزمون مستقل ۱ شماره مؤلفه: (ATE_IND.1.1D) شرح مؤلفه: توسعه دهنده باید برای آزمودن، محصول را ارائه نماید.

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
آزمون مستقل (ATE_IND)	نام عنصر: آزمون مستقل ۱ شماره مؤلفه: (ATE_IND.1.1C) شرح مؤلفه: محصول باید مناسب آزمودن باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
آزمون مستقل (ATE_IND)	نام عنصر: آزمون مستقل ۱ شماره مؤلفه: (ATE_IND.1.1E)

مؤلفه‌های اقدامات ارزیاب	
شرح مؤلفه:	
ارزیاب باید تائید نماید که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌نماید.	
نام عنصر: آزمون مستقل ۱	
شماره مؤلفه: (ATE_IND.1.2E)	
شرح مؤلفه:	
ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را آزمون نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.	

۷,۴ کلاس آسیب پذیری

۷,۴,۱ تحلیل آسیب پذیری

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	عنصر امنیتی
آسیب پذیری (AVA_VAN)	نام عنصر: آسیب پذیری ۱
	شماره مؤلفه: (AVA_VAN.1.1D)
	شرح مؤلفه:
	توسعه دهنده باید برای آزمون، محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
آسیب‌پذیری (AVA_VAN)	نام عنصر: آسیب‌پذیری ۱ شماره مؤلفه: (AVA_VAN.1.1C) شرح مؤلفه: محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
آسیب‌پذیری (AVA_VAN)	نام عنصر: آسیب‌پذیری ۱ شماره مؤلفه: (AVA_VAN.1.1E) شرح مؤلفه: ارزیاب باید تأیید نماید که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ شماره مؤلفه: (AVA_VAN.1.2E) شرح مؤلفه: ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ شماره مؤلفه: (AVA_VAN.1.3E) شرح مؤلفه:

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
	ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۷,۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پرو فایل حفاظتی ارائه شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه دهنده نقش کم‌رنگی در قابل اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۷,۵,۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، می‌باشد (بدین معنی که جدا از برچسب گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تأیید شده است را به آسانی تشخیص دهد.

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مؤلفه: (ALC_CMC.1.1D) شرح مؤلفه: توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مؤلفه: (ALC_CMC.1.1C) شرح مؤلفه: محصول باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی (ALC_CMC)	نام عنصر: برچسب گذاری محصول ۱ شماره مؤلفه: (ALC_CMC.1.1E) شرح مؤلفه: ارزیاب باید تأیید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۷,۵,۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMS)	نام عنصر: پوشش پیکربندی محصول ۱ شماره مؤلفه: (ALC_CMS.1.1D) شرح مؤلفه: ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMS)	نام عنصر: پوشش پیکربندی محصول ۱ شماره مؤلفه: (ALC_CMS.1.1C) شرح مؤلفه: لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ شماره مؤلفه: (ALC_CMS.1.1C) شرح مؤلفه: لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مؤلفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMS)	نام عنصر: پوشش پیکربندی محصول ۱ شماره مؤلفه: (ALC_CMS.1.1E) شرح مؤلفه: ارزیاب باید تأیید نماید که اطلاعات ارائه شده تمام مؤلفه های محتوایی را برآورده می نماید.

۸ پیوست یک: الزامات کلاس پشتیبانی از رمزنگاری مبتنی بر انتخاب

شماره الزام	نام الزام
۷۳	تولید کلید رمزنگاری ۱
محصول باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم های تولید کلید استاندارد زیر تولید کنند. [انتخاب: • <u>استفاده از طرح RSA با اندازه کلید 2048 بیت یا بیشتر که از این اسناد پیروی می کند: "Digital Signature Standard, FIPS PUB 186-4"</u> • <u>"Appendix B.3 (DSS)"</u> • <u>استفاده از طرح "NIST curves" ECC [انتخاب: P-256، P-384، P-521] که از اسناد زیر پیروی می کند: "Digital Signature Standard, FIPS PUB 186-4"</u> • <u>"Appendix B.4 Signature Standard (DSS)"</u> نکته کاربردی ۲۴: نویسنده سند هدف امنیتی تمام طرح های تولید کلید که برای استقرار و احراز هویت کاربران استفاده می شود را انتخاب می کند. وقتی کلید تولید شده برای احراز هویت کاربران استفاده می شود، انتظار می رود کلید عمومی با یک گواهی X.509v3 مرتبط گردد. در صورتیکه محصول به عنوان یک گیرنده در طرح استقرار کلید RSA عمل نماید، نیاز به پیاده سازی تولید کلید RSA نمی باشد.	
۷۴	تخریب کلید رمزنگاری ۱

شماره الزام	نام الزام
	محصول باید براساس متد تخریب کلید رمزنگاری [اختصاص: متد تخریب کلید رمزنگاری] که بر اساس استاندارد [اختصاص: لیستی از استانداردها] باشد، کلیدهای رمزنگاری را از بین ببرد. اقدامات تضمینی: • خلاصه مشخصات محصول ارزیاب باید این بخش را بررسی کند که در مورد همه کلیدهای محرمانه توضیحاتی بیان شده باشد. همچنین در مورد روش رویه تخریب کلید در حافظه (به عنوان مثال، بازنویسی با صفر و غیره) توضیحاتی را بیان نماید.
۷۵	عملیات رمزنگاری ۱- رمزنگاری و رمزگشایی (۳)
	محصول باید [رمزنگاری و رمزگشایی] را مطابق با الگوریتم رمزنگاری متقارن AES-XTS مطابق مستند NIST SP 800-38E، AES-CBC مطابق سند NIST SP 800-38A و [انتخاب : AES Key Wrap (KW) مطابق سند NIST SP 800-38F، AES Key Wrap with Padding (KWP) مطابق سند NIST SP 800-38F، AES-GCM مطابق سند NIST SP 800-38D، AES-CCM مطابق سند NIST SP 800-38C، و هیچکدام] با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد.

شماره الزام	نام الزام
نکته کاربردی ۲۵: انتخاب یک نوع و یا چند نوع از الگوریتم‌های مذکور به معماری و طراحی تولید کننده بستگی دارد.	
۷۶	عملیات رمزنگاری ۱ (۴) محصول مورد ارزیابی باید خدمات امضای دیجیتال (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب: • الگوی RSA: اندازه کلیدهای [انتخاب: ۲۰۴۸ بیتی یا بزرگ‌تر] و بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)» بخش ۴ • در مورد الگوی دیجیتال بیضوی ECDSA: اندازه کلیدهای [انتخاب: ۲۵۶ بیتی یا بزرگ‌تر] با استفاده از منحنی های NISTP-256 و P-384 و [انتخاب: P-521، هیچ منحنی دیگر]؛ بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۵] نکته کاربردی ۲۶: نویسنده هدف امنیتی باید الگوریتم مورد استفاده برای اجرای امضای دیجیتال را تعیین کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی باید انتخاب‌ها و اختصاص‌های مناسب را انجام دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین نماید.

۹ پیوست دو: الزامات پروتکل TLS مبتنی بر انتخاب

با استفاده از پروتکل‌های زیر می‌توان تهدیدات مرتبط با به خطر افتادن کانال ارتباطی بین مدیران و دیگر بخش‌های محصول یا موجودیت‌های IT خارجی را کاهش داد. برای حفاظت از اتصال سرور ممیزی و مدیران راه دور باید از یکی از پروتکل‌های ارتباطی امن (TLS/HTTPS, TLS) استفاده نمود.

شماره الزام	نام الزام
۷۷	الزامات پروتکل TLS Server / احراز هویت ۱
محصول باید [انتخاب: TLS 1.2 (RFC5246)] با پشتیبانی از مجموعه های رمز زیر را پیاده سازی نماید: • مجموعه های رمز اجباری: • [RFC 3268 TLS_RSA_WITH_AES_128_CBC_SHA مطابق با] • [انتخاب: مجموعه های رمز اختیاری: ○ LS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	

○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 • هیچ مجموعه رمز دیگری [[.	
نکته کاربردی ۲۷: مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدود شده‌اند. مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدود شده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.	
۷۸	الزامات پروتکل TLS Server / احراز هویت ۲
محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و [انتخاب: TLS1.1، هیچ‌کدام] دارند، رد نماید. نکته کاربردی ۲۸: تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در «الزامات پروتکل TLS Server / احراز هویت ۱» انتخاب‌نشده است، در اینجا انتخاب شود.	
۷۹	الزامات پروتکل TLS Server / احراز هویت ۳

محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [انتخاب: ۳۰۷۲ بیت، ۴۰۹۶ بیت، یا هیچ اندازه دیگری] و [انتخاب: منحنی‌های NIST [انتخاب: secp256r1, secp384r1] و هیچ منحنی دیگری]، [انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری] ایجاد نماید.

نکته کاربردی ۲۹:

اگر در بخش «الزامات پروتکل TLS Server / احراز هویت ۱» سند هدف امنیتی مجموعه رمزهای DHE یا ECDHE لیست شده باشند، سند ST باید شامل Diffie-Hellman یا منحنی‌های NIST لیست شده در این الزام باشد.