به نام خدا

سند هدف امنیتی

APKSWAP-V17.XX.XX

امن پردازان کویر

خرداد ماه ۱۴۰۱

نسخه۱,۲

فهرست

۱- معرفی سند هدف امنیتی

این بخش سند هدف امنیتی APKSWAP-V۱۷.XX.XX، شرکت امن‌پردازان کویر را معرفی می‌نماید. محصول APKSWAP که در این سند امنیتی ارائه شده؛ یک برنامه کاربردی تحت شبکه است که امکان مدیریت و ارتباط امن کاربران با سرور اینترنت را فراهم می‌سازد.

۱-۱- مرجع سند هدف امنیتی

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه مرورگر امن APKSWAP
نسخه	۱,۲
تاریخ	اردیبهشت ماه ۱۴۰۱
نویسندگان	گروه توسعه APKSWAP شرکت امن پردازان کویر

۱-۲- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	شرکت امن پردازان کویر
نام محصول	APKSWAP
نوع محصول	برنامه کاربردی تحت شبکه
نسخه	۱۷.XX.XX

۱-۲-۱- نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی

محصول APKSWAP به عنوان یک برنامه کاربردی تحت شبکه با استفاده از سرویس‌ها و تنظیمات مورد نیاز، محیطی را جهت ارتباط امن کاربران به شبکه اینترنت فراهم می‌نماید. تمامی بخش‌های مورد نیاز بر روی سرور مجازی نصب می‌گردند. در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای کارکرد محصول بیان شده است:

کامپوننت‌ها	حداقل الزامات
پردازنده	۲ *Intel® Xeon® E۵-۲۶۹۰v۴ (۲.۶GHz/۱۴-core/۳۵MB/۱۳۵W)
سیستم عامل	Linux Ubuntu Server
....	...

۱-۳- توصیف هدف ارزیابی

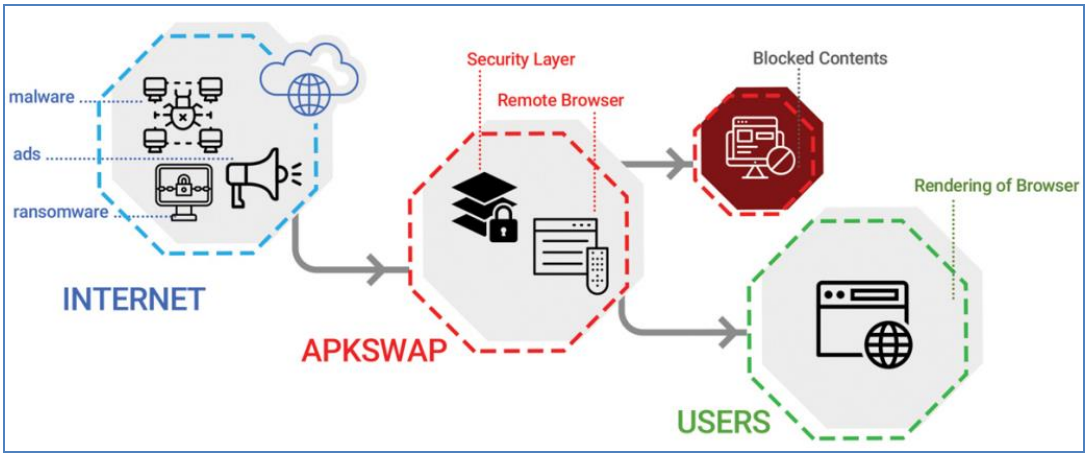
۱-۳-۱- حوزه فیزیکی

عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می‌شود:

عناصر محصول	شماره مدل یا نسخه
Linux Ubuntu Server	۲۰.۰۴.XX LTS
Docker	XX.XX.XX

در این جدول لازم است هرمؤلفه ی که در شکل محیط عملیاتی با محصول در ارتباط است از جمله تمام سرورها و... در این جدول ذکر شوند.

در این بخش قرار گیری محصول در محیط عملیاتی و پیکربندی آن در قالب تصویر آورده شود. لازم است محصول و محیط عملیاتی به تفکیک در تصویر مشخص گردند.



۱-۳-۲- حوزه منطقی

کارکردهای امنیتی هدف ارزیابی تحت عنوان حوزه منطقی شناخته می‌شود که باید به صورت مشخص هریک از کارکردها و شرح آنها در این قسمت مطرح شود.

کارکردها	توصیف
احراز هویت با استفاده از سرویس Active Directory	ارتباط نرم افزار با سرور Active Directory و شناسایی هویت فرد
کنترل دسترسی	هدف ارزیابی دارای امکان دسترسی محدود میباشد، به طوریکه تنها موجودیت های مجاز خاص دارای دسترسی به داده و کارکردهای هدف ارزیابی هستند.برای کاربران مجاز کنترل دسترسی معمولا با استفاده از داده احراز هویت انجام میگیرد
Login به نرم افزار با استفاده از Web service	ارتباط نرم افزار با Web Serviceو شناسایی هویت فرد
رویداد نگاری	مشاهده تمامی فعالیت های انجام شده توسط کاربران
حوزه رمزنگاری	هدف ارزیابی از انواع الگوریتم های رمزنگاری متقارن و نامتقارن پشتیبانی می کند.
مدیریت دسترسی در محصول	فقط کاربران تعریف شده در محدوده های مجوزهای داده شده می‌توانند به امکانات مدیریتی سامانه دسترسی داشته باشند.
ایجاد ارتباط امن	برقراری ارتباط امن به منظور دسترسی به شبکه اینترنت را فراهم می‌کند

۲- ادعای انطباق

۲-۱- انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	این سند هدف امنیتی منطبق بر استاندارد ارزیابی معیار مشترک است ISO/IEC ۱۵۴۰۸, version ۳.۱, revision ۵,۲۰۱۷
انطباق با SFRها (قسمت دوم از CC)	این سند هدف امنیتی توسعه یافته است.
انطباق با SARها (قسمت سوم از CC)	این سند هدف امنیتی منطبق بر قسمت سوم از استاندارد ارزیابی معیار مشترک است.

۲-۲- انطباق با پروفایل حفاظتی

نام پروفایل حفاظتی	پروفایل حفاظتی برنامه کاربردی تحت شبکه نسخه ۱,۱ اسفند ماه ۹۶

۲-۳- انطباق با سطح تضمین امنیتی

سطح تضمین امنیتی	این سند جهت تطابق هدف ارزیابی با EAL۱ ارائه گردیده است.

۳- تعریف مسائل امنیتی

۳-۱- خط‌مشی

خط مشی ها	توضیحات
P.COMPLEMENTARY_AUDIT	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.
P.PROPER_CONFIGURATION	پیکربندی پیش‌فرض محصول و مولفه‌های تعاملی تحت کنترل محصول باید تغییر

خط مشی ها	توضیحات
	یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس‌هایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیش‌فرض، خطاهای پیش‌فرض و صفحات ۴۰۴، مقادیر احراز هویت پیش‌فرض، نام کاربری پیش‌فرض، پورت‌های پیش‌فرض، صفحات پیش‌فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می‌نمایند. این خط‌مشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار می‌گیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی می‌توان از حمله‌ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
P.E_SIGNATURE	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۳-۲- تهدیدات

تهدیدات	توضیحات
T.UNAUTHORIZED_ACCESS	مهاجم می‌تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی می‌تواند با استفاده 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 تست 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.
T.DATA_ALTERATION	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 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.
T.REPUDIATION	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.

تهدیدات	توضیحات
T.DATA_DISCLOSURE	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.
T.DENIAL_OF_SERVICE	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 می-گیرد طوریکه 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.
T.HARMFUL_DATA	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 رابه دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
T.ELEVATION_OF_PRIVILEGES	مهاجم می‌تواند با سود بردن از دسترسی غیرمجاز، ورود داده‌های مخرب و تغییر داده‌ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.
T.NETWORK_EAVESDROP	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می‌شود تا انتقال داده‌های حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده‌های رد و بدل شده بین محصول و یک یا چند کاربر از راه دور و یا محلی است. به عنوان مثال می‌توان به موردی اشاره کرد که در آن یک کاربر تلاش می‌کند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد می‌نماید.

۳-۳- فرضیات

فرضیات	توضیحات
A.TRUSTED_ADMIN	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
A.TRUSTED_DEVELOPER	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 می‌نمایند.
A.EXPERIENCED_ DEVELOPER	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب‌پذیری‌های شناخته شده را اتخاذ می‌نمایند.
A.SECURE_ENVIRONMENT	فرض شده است که تمام پیش‌بینی‌های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری

فرضیات	توضیحات
	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 می‌گیرد.
A.PROPER_BACKUP	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره-سازی و دیگر مولفه‌های سخت‌افزاری دارای پشتیبان مناسبی هستند، و بنابر وجود نسخه پشتیبان هیچ داده‌ای از دست نمی‌رود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمی‌دهد.
A.COMMUNICATION	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 درقبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می‌شوند.
A.SECURE_DELIVERY	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.
A.DIST_DENIAL_OF_SERVICE	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.

۴- اهداف امنیتی

۴-۱- اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توضیحات
O.AUDIT	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.

هدف امنیتی	توضیحات
O.AUTH	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 می‌نماید. 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 احرازهویت نماید. از جمله سازوکارها می‌توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احرازهویت براساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روش‌ها اشاره نمود.
O.DATA_FLOW_CONTROL	محصول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست‌ها از یک رنج IP تعریف شده می‌تواند 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.
O.DATA_INTEGRITY	محصول باید نسبت به صحت داده ممیزی و داده‌ی رکورد با تشخیص هرگونه تغییر بر روی این داده‌ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
O.MANAGEMENT	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارامد سیستم فراهم نماید. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسط‌های 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.
O.ERROR_MANAGEMENT	محصول باید صورت امن و کارامد 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 خطا 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.

هدف امنیتی	توضیحات
O.RESIDUAL_DATA_MNG	محصول باید اطمینان دهد که هر داده‌ی باقیمانده از محصول زمانیکه دیگر بـه آن نیـاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس می‌گردد.
O.TLS_Communication	تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

۴-۲- اهداف امنیتی برای محیط عملیاتی

اهداف امنیتی محیطی	توضیحات
OE.SECURE_ENVIRONMENT	محیط عملیاتی محصول باید نسبت بـه امنیـت محیطـی و فیزیکـی محصـول اطمینـان دهـد. دسترسی غیرمجاز باید محدود گردیده و تمام مولفه‌ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مولفه‌های حساس را داشته باشند. محیط عملیاتی محصـول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظـت شـده است. از جمله سازوکارهای حفاظتی می‌توان به غیرفعال نمودن سرویس‌هـا، پـورت‌هـا و دیگـر موارد استفاده شده اشاره نمود.
OE.COMMUNICATION	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌هـای ارتبـاطی امـن بایـد فـراهم گردد.
OE.TRUSTED_ADMIN	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آمـوزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
OE.TRUSTED_DEVELOPER	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آمـوزش کـافی دیده و الزامات امنیتی را برآورده می‌نمایند.
OE. EXPERIENCED_DEVELOPER	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهنده‌ی محصـول در زمینـه امنیت تجربه داشته و آنها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتـی شـناخته شده را در نظر می‌گیرد.
OE.COMPLEMENTARY_AUDIT	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیـزی بـرای محـیط عملیاتی محصول می‌باشد. رکوردهای ممیزی محصول در صورت ترکیـب بـا بـاقی رکوردهـای ممیزی بسیار معنادار خواهند بود.
OE. SECURE_DELIVERY	تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شـود. علـاوه بر این، کارکردها و/یا پارامترهای استفاده شده به منظور تست باید پاک یا غیر قابـل دسـترس گردند.
OE. PROPER_BACKUP	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمـام داده‌هـای باقیمانـده در محیط عملیاتی محصول را حفظ نماید. برای ایـن منظـور ممکـن اسـت از روال‌هـای از پـیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مولفه‌هـای سـخت-افزاری نیز نسخه پشتیبان تهیه گردد.

۵- نیازمندی‌های امنیتی

۵-۱- الزامات کارکرد امنیتی

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۱	کلاس ممیزی امنیت	تولید داده ممیزی ۱	FAU_GEN.۱.۱
۲		تولید داده ممیزی ۲	FAU_GEN.۱.۲
۳		مرتبط نمودن هویت کاربر به رویداد ۱	FAU_GEN.۲.۱
۴		بازبینی داده ممیزی ۱	FAU_SAR.۱.۱
۵		بازبینی داده ممیزی ۲	FAU_SAR.۱.۲
۶		بازبینی داده ممیزی محدود ۱	FAU_SAR.۲.۱
۷		بازبینی داده ممیزی قابل انتخاب ۱	FAU_SAR.۳.۱
۸		انتخاب داده ممیزی ۱	FAU_SEL.۱.۱
۹		ذخیره‌سازی رویدادهای ممیزی ۱	FAU_STG.۱.۱
۱۰		ذخیره‌سازی رویدادهای ممیزی ۲	FAU_STG.۱.۲
۱۱		اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	FAU_STG.۳.۱
۱۲		پیشگیری از اتلاف و از بین رفتن داده ممیزی ۱	FAU_STG.۴.۱
۱۳	کلاس پشتیبانی از رمزنگاری	عملیات رمزنگاری ۱ (۱) (یکپارچگی داده‌های رکورد و داده‌های ممیزی)	FCS_COP.۱.۱(۱)
۱۴		عملیات رمزنگاری ۱ (۲) (تولید مقادیر **hash**)	FCS_COP.۱.۱(۲)
۱۵	کلاس حفاظت از داده کاربری	خط‌مشی کنترل دسترسی ۱	FDP_ACC.۱.۱
۱۶		عملیات کنترل دسترسی ۱	FDP_ACF.۱.۱
۱۷		عملیات کنترل دسترسی ۲	FDP_ACF.۱.۲
۱۸		عملیات کنترل دسترسی ۳	FDP_ACF.۱.۳
۱۹		عملیات کنترل دسترسی ۴	FDP_ACF.۱.۴
۲۰		حفاظت کامل از اطلاعات باقیمانده در منابع ۱	FDP_RIP.۲.۱
۲۱		صحت داده کاربری ذخیره شده ۲	FDP_SDI.۲.۱
۲۲		صحت داده کاربری ذخیره شده ۳	FDP_SDI.۲.۲
۲۳	کلاس شناسایی و احرازهویت	مدیریت احرازهویت ناموفق ۱	FIA_AFL.۱.۱
۲۴		مدیریت احرازهویت ناموفق ۲	FIA_AFL.۱.۲
۲۵		تعریف مشخصات کاربر ۱	FIA_ATD.۱.۱
۲۶		مدیریت کلمه عبور	FIA_PMG_EXT.۱.۱

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۲۷		احرازهویت کاربر ۱	FIA_UAU.۱.۱
۲۸		احرازهویت کاربر ۲	FIA_UAU.۱.۲
۲۹		سازوکار احرازهویت چندگانه ۱	FIA_UAU.۵.۱
۳۰		سازوکار احرازهویت چندگانه ۲	FIA_UAU.۵.۲
۳۱		شناسایی کاربر ۱	FIA_UID.۱.۱
۳۲		شناسایی کاربر ۲	FIA_UID.۱.۲
۳۳		انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱	FIA_USB.۱.۱
۳۴		انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.۱.۲
۳۵		انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.۱.۳
۳۶	کلاس مدیریت امنیت	مدیریت کارکرد در محصول ۱	FMT_MOF.۱.۱
۳۷		مدیریت مشخصه‌های امنیتی ۱	FMT_MSA.۱.۱
۳۸		مدیریت مشخصه‌های امنیتی ۳	FMT_MSA.۳.۱
۳۹		مدیریت مشخصه‌های امنیتی ۴	FMT_MSA.۳.۲
۴۰		مدیریت داده‌های محصول ۱ – مدیر سیستم	FMT_MTD.۱.۱ (۱)
۴۱		مدیریت داده‌های محصول ۱ – کاربر عادی، وارد کننده داده	FMT_MTD.۱.۱ (۲)
۴۲		کارکردهای مدیریتی محصول ۱	FMT_SMF.۱.۱
۴۳		نقش‌های امنیتی ۱	FMT_SMR.۱.۱
۴۴		نقش‌های امنیتی ۲	FMT_SMR.۱.۲
۴۵	کلاس حفاظت از توابع امنیتی محصول	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.۱.۱
۴۶		سازگاری داده امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.۱.۱
۴۷		سازگاری داده امنیتی بین محصول و موجودیت امن ۲	FPT_TDC.۱.۲
۴۸	کلاس تخصیص منابع	تحمل خطا ۱	FRU_FLT.۱.۱
۴۹	کلاس دسترسی به محصول	محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.۱.۱
۵۰		محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.۱.۲
۵۱		خاتمه دادن به نشست ها توسط محصول ۱	FTA_SSL.۳.۱
۵۲		خاتمه دادن به نشست ها توسط کاربر ۱	FTA_SSL.۴.۱
۵۳		سوابق دسترسی به محصول ۱	FTA_TAH.۱.۱
۵۴		برقراری نشست ۱	FTA_TSE.۱.۱
۵۵	کلاس کانال‌های/مسیرهای مورد اعتماد	کانال امن ۱	FTP_ITC.۱.۱
۵۶		کانال امن ۲	FTP_ITC.۱.۲
۵۷		کانال امن ۳	FTP_ITC.۱.۳
۵۸		مسیر امن ۱	FTP_TRP.۱.۱

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۵۹		**مسیر امن ۲**	FTP_TRP.۱.۲
۶۰		**مسیر امن ۳**	FTP_TRP.۱.۳
		الزامات پیوست یک **الزامات پیوست دو**	
۶۱	**الزامات پروتکل HTTPS**	**الزامات پروتکل HTTPS (۱)**	FCS_HTTPS_EXT.۱.۱
۶۲		**الزامات پروتکل HTTPS (۲)**	FCS_HTTPS_EXT.۱.۲
۶۳		**الزامات پروتکل HTTPS (۳)**	FCS_HTTPS_EXT.۱.۳
۶۴	**الزامات پروتکل TLS Client**	**الزامات پروتکل TLS Client (۱)**	FCS_TLSC_EXT.۱.۱
۶۵		**الزامات پروتکل TLS Client (۲)**	FCS_TLSC_EXT.۱.۲
۶۶		**الزامات پروتکل TLS Client (۳)**	FCS_TLSC_EXT.۱.۳
۶۷	**الزامات پروتکل TLS Server**	**الزامات پروتکلTLS Server (۱)**	FCS_TLSS_EXT.۱.۱
۶۸		**الزامات پروتکلTLS Server (۲)**	FCS_TLSS_EXT.۱.۲
۶۹		**الزامات پروتکلTLS Server (۳)**	FCS_TLSS_EXT.۱.۳
۷۰	**الزامات شناسایی و احرازهویت**	**الزامات پروتکل X۵۰۹ (۱) / ابطال**	FIA_X۵۰۹_EXT.۱.۱/Rev
۷۱		**الزامات پروتکل X۵۰۹ (۲) / ابطال**	FIA_X۵۰۹_EXT.۱.۲/Rev
۷۲		**الزامات پروتکل X۵۰۹ (۳)**	FIA_X۵۰۹_EXT.۲.۱
۷۳		**الزامات پروتکل X۵۰۹ (۴)**	FIA_X۵۰۹_EXT.۲.۲

۵-۱-۱- کلاس ممیزی امنیت

<table>
<tr><th>مؤلفه</th><th>وابستگی ها</th><th>شماره</th><th>المان</th><th>شرح المان</th></tr>
<tr><td>FAU_GEN.۱</td><td>FPT_STM.۱</td><td>۱</td><td>FAU_GEN.۱.۱</td><td>محصول باید بر اساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید کند:
• آغاز و اتمام توابع ممیزی
• تمامی رویدادهای قابل ممیزی (برای نوع داده حساس و داده‌هایی که بار حقوقی دارند) که در جدول ۱ آمده است.
<table>
<tr><th>مولفه</th><th>رویداد قابل ممیزی</th><th>جزئیات</th></tr>
<tr><td>مرتبط نمودن هویت کاربر به رویداد ۱</td><td>تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)</td><td></td></tr>
<tr><td>بازبینی داده ممیزی ۱</td><td>خواندن اطلاعات از رکوردهای ممیزی (پایه)</td><td></td></tr>
<tr><td>انتخاب داده ممیزی ۱</td><td>ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می‌افتد در حالی‌که توابع ممیزی در حال انجام عملیات باشند. (حداقل)</td><td></td></tr>
<tr><td>اقدامات لازم در زمان از دست رفتن داده ممیزی ۱</td><td>عملیات انجام شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)</td><td></td></tr>
<tr><td>پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۱</td><td>عملیات انجام شده به دلیل شکست ذخیره‌سازی ممیزی (پایه)</td><td></td></tr>
<tr><td>صحت داده های کاربری ذخیره شده ۲</td><td>تلاش‌های موفقیت‌آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل)
تمامی تلاش‌ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)</td><td></td></tr>
<tr><td>احراز هویت کاربر</td><td>ثبت کاربرد ناموفق از سازوکار احرازهویت (حداقل)
ثبت تمام کاربردهای سازوکار احراز هویت (پایه)</td><td></td></tr>
</table></td></tr>
</table>

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				سازوکار احرازهویت چندگانه	ثبت نتایج احرازهویت (حداقل) ثبت هر سازو کار احرازهویت فعال همراه با نتیجه نهائی (پایه)	
				شناسایی کاربر	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبداء، شناسایی نقطه پایانی اتصال
				مدیریت کلمه عبور	ثبت رد هر کلمه عبور تست شده توسط محصول (حداقل) ثبت تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول (پایه)	برای مثال، رد و یا قبول کلمه عبور کاربر
				انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	ثبت شکست انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل) شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه)	
				مدیریت مشخصه‌های امنیتی	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی (پایه)	
				مدیریت داده های محصول ۱-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
						رکوردها و اسناد باید ثبت شود.
				مدیریت داده های محصول ۱- کاربرعادی، وارد کننده داده	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
				عملیات رمزنگاری ۱(۱)	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)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیر فعال (پایه)	
				عملیات کنترل دسترسی ۱	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)	شناسایی داده‌های موجودیت غیرفعال
				ورود داده‌های کاربری به محصول با	ورود داده کاربری موفقیت آمیز، شامل هر گونه	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				مشخصه امنیتی	مشخصه‌های امنیتی (حداقل) تمامی تلاش‌ها برای وارد کردن داده‌های کاربری، شامل هر گونه مشخصه‌های امنیتی (پایه)	
				خروج داده های کاربری از محصول با مشخصه امنیتی	خروج اطلاعات به‌طور موفقیت‌آمیز (حداقل) همه تلاش‌ها برای خارج کردن اطلاعات از محصول (پایه)	
				مدیریت کارکرد در محصول	تمامی تغییرات در رفتارهای کارکردی محصول	
				کارکردهای مدیریتی محصول	ثبت استفاده از کارکردهای مدیریتی (حداقل)	
				نقش‌های امنیتی	ثبت تغییرات در گروه‌های کاربری که بخشی از یک نقش می‌باشد (حداقل)	
				سازگاری داده‌های امنیتی بین محصول و موجودیت امن	ثبت استفاده موفق از مکانیزم سازگاری داده‌های محصول (حداقل) ثبت استفاده از مکانیزم سازگاری داده‌های محصول (پایه)	
				حفظ وضعیت امن در زمان شکست	ثبت شکست در محصول (پایه)	
				تحمل خطا	ثبت هر شکست شناسایی شده توسط محصول (حداقل) ثبت تمامی قابلیت‌های در حال قطع شدن محصول که به دلیل شکست می‌باشد (پایه)	
				برقراری نشست ۱	ثبت منع آغاز نشست بدلیل مکانیزم آغاز نشست (حداقل) ثبت تمامی تلاش‌ها در آغاز نشست کاربر (پایه)	
				محدودیت بر روی چندین نشست	ثبت رد یک نشست مبتنی بر محدودیت	

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
				همزمان	نشست‌های 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)	

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		۲	**FAU_GEN.1.2**	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 [**هر نوع اطلاعات قابل ممیزی دیگر از قبیل آدرس IP کاربر، نام و شناسه کاربری، نسخه سیستم عامل، زمان و تاریخ انجام فعالیت**] .
FAU_GEN.۲	**FAU_GEN.۱** **FIA_UID.۱**	۳	**FAU_GEN.۲.۱**	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.
FAU_SAR.۱	**AU_GEN.۱**	۴	**FAU_SAR.۱.۱**	محصول باید امکان خواندن **[اطلاعات ممیزی مربوط به ورود و خروج موفق و ناموفق کاربران، ایجاد-حذف-ویرایش-مشاهده اطلاعات ممیزی و کلیه تنظیمات سامانه]** را برای **[کاربران مجاز]** فراهم نماید.
		۵	**FAU_SAR.۱.۲**	محصول باید رکوردهای ممیزی را طوری فراهم نماید که کاربر بتواند آن‌ها را درک و اطلاعات این رکوردها را تفسیر کند.
FAU_SAR.۲	**FAU_SAR.۱**	۶	**FAU_SAR.۲.۱**	محصول باید مانع دسترسی خواندن رکوردهای ممیزی توسط کلیه کاربران به غیر از کاربرانی که به صورت صریح مجاز به دسترسی خواندن هستند، گردد.
FAU_SAR.۳	**FAU_SAR.۱**	۷	**FAU_SAR.۳.۱**	محصول باید امکان انجام [**متدهای انتخاب و مرتب‌سازی**] رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را بر اساس [**حساب کاربری، تاریخ/زمان، مکان، روش اتصال کاربر، درجه اهمیت رکوردها، نوع رخداد و هیچ پارامتر دیگری**] مرتب کند.
FAU_SEL.۱	**FAU_GEN.۱** **FMT_MTD.۱**	۸	**FAU_SEL.۱.۱**	محصول باید قادر باشد بر اساس مشخصه‌های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادها را جهت ممیزی شدن، انتخاب نماید: [نوع رخداد] **[هیچ معیار انتخاب دیگری]**.
FAU_STG.۱	**FAU_GEN.۱**	۹	**FAU_STG.۱.۱**	محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره‌سازی را، از حذف غیرمجاز حفاظت نماید.
		۱۰	**FAU_STG.۱.۲**	محصول باید قادر به [تشخیص] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره‌سازی آن‌ها باشد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_STG.۳	**FAU_STG.۱**	۱۱	**FAU_STG.۳.۱**	محصول در صورت تجاوز دنباله ممیزی از **[یک محدودیت از پیش تعریف شده]** باید با استفاده از **[یک کانال ارتباطی، پیام کوتاه یا معادل آن، از طریق واسطهای محصول کاربران مربوطه را]** مطلع نماید.
FAU_STG.۴	**FAU_STG.۱**	۱۲	**FAU_STG.۴.۱**	محصول در صورت پر شدن دنباله ممیزی، باید[روی قدیمی ترین رکوردهای ممیزی ذخیره شده دوباره نویسی نماید.] و **[به شماره وارد شده توسط مدیر سیستم پیامک هشدار ارسال کند]**.

۵-۱-۲- کلاس پشتیبانی از رمزنگاری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_COP.۱	FDP_ITC.۱ FCS_CKM.۴	۱۳	**FCS_COP.۱.۱(۱)**	محصول باید **[برای وارسی صحت دادههای ممیزی و دادههای رکورد]** بر اساس یک الگوریتمهای رمزنگاری مشخص **[RSA]** و اندازه کلید رمزنگاری**[۵۱۲ بیت و ۲۵۶ بیت]** اجرا میشود که مطابق استاندارد **[SHA۲۵۶]** باشد.
FCS_COP.۱	FDP_ITC.۱ FCS_CKM.۴	۱۴	**FCS_COP.۱.۱(۲)**	محصول باید **[تولید داده درهمسازی]** بر اساس یک الگوریتمهای رمزنگاری مشخص **[AES]** و اندازه کلید رمزنگاری**[۲۵۶ بیت]** اجرا میشود که مطابق استاندارد**[aes-۲۵۶-cbc]** باشد.

۵-۱-۳- کلاس حفاظت از داده کاربری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.۱	FDP_ACF.۱	۱۵	**FDP_ACC.۱.۱**	محصول باید خطمشیهای کنترل دسترسی را بر روی موارد زیر اعمال کند: **]** ▪ **موجودیت فعال:**[**مدیر سیستم، کاربر عادی، هیچ موجودیت فعال دیگری**] **موجودیت غیرفعال:**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				▪ رکوردها، مستندات و فراداده ▪ داده متعلق به کاربران ▪ داده احرازهویت ▪ داده با این معیار ها:[تنظیمات،محدودیت بر اساس زمان، محدودیت بر اساس IP] ▪ اختصاص: [داده متعلق به گروه کاربری، داده متعلق به برنامه های کاربردی] عملیات: ▪ ایجاد موجودیت غیرفعال جدید ▪ حذف موجودیت غیرفعال ▪ تغییر دسترسی‌ها به موجودیت غیرفعال ▪ عملیات بر روی فراداده وابسته به موجودیت غیرفعال ▪ [تغییر رمز عبور کاربران، مشاهده موجودیت های فعال و غیر فعال، آپدیت موجودیت های فعال و غیر فعال]]

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FDP_ACC.۱	FDP_ACC.۱ FMT_MSA.۳	۱۶	**FDP_ACF.۱.۱**	محصول باید [**خط‌مشی‌های کنترل دسترسی**] را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید: [• **هویت کاربر** • **نقش‌ها و مجوزهای کاربر مجاز** • **اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.** • **[هیچ مشخصه موجودیت فعال دیگری]**]
		۱۷	**FDP_ACF.۱.۲**	محصول باید قوانین زیر را اجرا نماید تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید: **[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.]**
		۱۸	**FDP_ACF.۱.۳**	محصول باید بر اساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال دارا می‌باشد: [• **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.** • **[هیچ قانون دیگری]**]
		۱۹	**FDP_ACF.۱.۴**	محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری می‌کند:

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				] • **تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف شده،** • **[هیچ قانون دیگری]** [
FDP_RIP.۲	-	۲۰	**FDP_RIP.۲.۱**	محصول باید تضمین نماید در هنگام [آزادسازی منابع]از تمام موجودیت‌های غیرفعال استفاده شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.
FDP_SDI.۲	-	۲۱	**FDP_SDI.۲.۱**	محصول باید داده کاربری حساس و یا دارای بار حقوقی ذخیره شده در مکان تحت کنترل خود را برای تشخیص [**خطاهای صحت داده**] داده‌های رکورد و داده‌های ممیزی را بر اساس مشخصه‌های[**درهم شده داده‌های کاربری ذخیره شده**] پایش نماید.
		۲۲	**FDP_SDI.۲.۲**	هنگام تشخیص خطای صحت داده، محصول باید**[نمایش در رابط کاربری عدم صحت داده]** را صورت دهد.

۵-۱-۴- کلاس شناسایی و احرازهویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_AFL.۱	**FIA_UAU.۱**	۲۳	**FIA_AFL.۱.۱**	محصول باید بتواند با استفاده از **[[یک عدد مثبت]** قابل تنظیم توسط مدیر **[بازه ۱ تا ۲۰]]** ، تلاش‌های ناموفق احراز هویت مرتبط با**[احراز هویت در صفحه‌ی ورود]** را تشخیص دهد.
		۲۴	**FIA_AFL.۱.۲**	زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به[حد تعیین شده رسید]، محصول باید**[بررسی captcha]** را اجرا کند که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.
FIA_ATD.۱	-	۲۵	**FIA_ATD.۱.۱**	محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید: **]** • **شناسه کاربر**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• **متد احرازهویت مورد استفاده** • **داده احرازهویت** • **نقش کاربر** • **وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)** • **[هیچ مشخصه امنیتی دیگر]**]
FIA_PMG_EXT.۱	-	۲۶	**FIA_PMG_EXT.۱.۱**	محصول باید قابلیت‌های مدیریت کلمه عبور را که در زیر ذکر شده‌اند برای کلمه‌های عبور مدیریتی فراهم کند: • کلمه عبور باید بتواند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: ["@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" , ")"] باشد. • حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و ۸ کاراکتر یا بیشتر باشد.
FIA_UAU.۱	**FIA_UID.۱**	۲۷	**FIA_UAU.۲.۱**	محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احرازهویت نماید.

۵-۱-۵- کلاس مدیریت امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MOF.۱	FMT_SMR.۱ FMT_SMF.۱	۲۸	**FMT_MOF.۱.۱**	محصول باید امکان [فعال نمودن، غیرفعال نمودن] تمام توابع [**تمام کارکردهای مربوط به مدیریت محصول]** را به **[مدیر سیستم و هر کاربری که مجوز لازم را دارد ،[هیچ نقش دیگری]]** محدود کند.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MSA.۱	FDP_ACC.۱ FMT_SMR.۱ FMT_SMF.۱	۲۹	**FMT_MSA.۱.۱**	• محصول باید با اعمال **[خط‌مشی کنترل دسترسی]**، امکان تغییر پیش‌فرض، پرس و جو، تغییر، حذف، **[هیچ عملیات دیگری]** مشخصه‌های امنیتی **[** • **شناسه کاربر** • **نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت (جزئیات تلاش برای احرازهویت موفق و ناموفق)** • **[نام کاربری، IP سیستم کاربر، تاریخ ورود]]** را به **[مدیر سیستم و هر کاربری که مجوز لازم را دارد]** محدود نماید.
FMT_MSA.۳	FMT_MSA.۱ FMT_SMR.۱	۳۰	**FMT_MSA.۳.۱**	محصول برای مشخصه‌های امنیتی که برای اعمال **[خط مشی]** استفاده می‌شوند، باید مقادیر پیش فرض محدود شده‌ای درنظر بگیرد.
		۳۱	**FMT_MSA.۳.۱**	محصول برای تعیین مقادیر اولیه پیشنهادی باید به **[مدیر سیستم]** اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیر فعال، مقادیر پیش‌فرض را لغو و تغییر دهد.
FMT_MTD.۱	FMT_SMR.۱ FMT_SMF.۱	۳۲	**FMT_MTD.۱.۱ (۱)**	محصول باید توانایی پرس‌وجو، تغییر، حذف، پاک نمودن، **[مشاهده، ایجاد]** **[** • **داده های ممیزی** • **تنظیمات امنیتی سامانه** • **داده‌های احراز هویت** **]** را به **[مدیر سیستم،[هیچ نقش دیگری]**] محدود نماید.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MTD.1		۳۳	**FMT_MTD.1.1 (۲)**	محصول باید توانایی **[مشاهده، استفاده]** **]** • **برنامه های کاربردی** • **اخرین بازدید** **[** را به **[کاربر عادی]** محدود نماید.
FMT_SMF.1	-	۳۴	**FMT_SMF.1.1**	محصول باید قادر به انجام **[کارکردهای مدیریتی که در جدول زیر آمده است]** باشد:

مولفه استاندارد	مولفه	عملیات مدیریتی
FAU_SAR.۱	بازبینی داده ممیـزی 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	انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزاد سازی) که می‌تواند در محصول قابل

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
					منابع	پیکربندی باشد.
					ورود داده های کاربری به محصول با مشخصه امنیتی	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
					صحت داده های کاربری ذخیره شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد.
					مدیریت احراز هویت ناموفق	مدیریت حدآستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.
					مدیریت کلمه عبور	مدیریت تنظیمات و الزامات و قابلیت‌ها برای تنظیم کلمه عبورها
					احراز هویت کاربر	مدیریت داده‌های احرازهویت توسط مدیر یا کاربر مرتبط مدیریت یکسری عملیاتی که قبل از احرازهویت کاربر انجام می‌شوند.
					سازوکار احرازهویت چندگانه	مدیریت سازوکارهای احرازهویت مدیریت قوانین مرتبط با احرازهویت
					شناسایی کاربر	مدیریت تغییرات و فرایندهایی مانند(اختصاص ادرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر

مؤلفه	وابستگی ها	شماره	المان	شرح المان		
						مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.
				انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر		مدیر مجاز می‌تواند مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف و تغییر دهد.
				مدیریت مشخصه‌های امنیتی		مدیریت گروهی از نقش‌هایی که با مشخصه‌های امنیتی در تعامل هستند.
				مقدار دهی اولیه مشخصه‌ها		مدیریت گروهی از نقش‌هایی که مقادیر اولیه را مشخص می-کنند. مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول
				مدیریت داده های محصول ۱-مدیر سیستم		مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
				مدیریت داده های محصول ۱- کاربرعادی، وارد کننده داده		مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
				نقش‌های امنیتی		مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
				محدودیت بر روی چندین نشست		مدیریت حداکثر نشست مجاز کاربران به طور همزمان توسط مدیر

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				همزمان 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. تعیین زمان پیش‌فرض غیرفعال بودن کاربر که نشست خاتمه یابد.
FMT_SMR.۱	FIA_UID.۱	۳۵	**FMT_SMR.۱.۱**	نقش‌های زیر در محصول باید تعریف شده باشد: مدیر سیستم، کاربر عادی، [نقش های تعریف شده توسط مدیر سیستم]
		۳۶	**FMT_SMR.۱.۲**	محصول باید قادر به مرتبط نمودن کاربران با نقش‌ها و دسترسی‌های مجاز تعریف شده باشند.

۵-۱-۶- کلاس حفاظت از توابع امنیتی محصول

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPT_FLS.۱	-	۳۷	**FPT_FLS.۱.۱**	محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: **[شکست‌های نرم‌افزاری، شکست‌های سخت‌افزاری]**
FPT_TDC.۱	-	۳۸	**FPT_TDC.۱.۱**	محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار [**داده احراز هویت، داده پنل پیامکی**] را در زمان اشتراک‌گذاری داده امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد.
FPT_TDC.۱	-	۳۹	**FPT_TDC.۱.۲**	محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، **]** • **کد احرازهویت دو مرحله‌ای**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• **ورود موفق یا ناموفق کاربر**] استفاده نماید.
FTA_TUD_EXT.۱	افتا	۴۰	**FTA_TUD_EXT.۱.۲**	محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کارشناس شرکت تولید کننده محصول فراهم نماید که به‌روزرسانی نرم‌افزار و میان‌افزارمحصول مورد ارزیابی را به صورت دستی آغاز نماید و[از هیچ مکانیسم به‌روزرسانی پشتیبانی نکند.]

۵-۱-۷- کلاس تخصیص منابع

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FRU_FLT.۱	FPT_FLS.۱	۴۱	**FRU_FLT.۱.۱**	محصول باید از عملکرد تمام کارکردهای اصلی هنگام رویداد شکست‌های زیر اطمینان حاصل می‌کند: **[شکست نرم‌افزاری، [هیچ شکست دیگری]]**

۵-۱-۸- کلاس دسترسی به محصول

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_MCS.۱	FIA_UID.۱	۴۲	**FTA_MCS.۱.۱**	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود کند.
			FTA_MCS.۱.۲	محصول باید به صورت پیش‌فرض، **[تعداد نشست همزمان پیش‌فرض یک]** برای هر کاربر در نظر بگیرد.
FTA_SSL.۳	-	۴۳	**FTA_SSL.۳.۱**	محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمان **[بازه زمانی که توسط مدیر تنظیم می‌شود]** غیرفعال بودن، خاتمه دهد.
FTA_SSL.۴	-	۴۴	**FTA_SSL.۴.۱**	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_TAH.۱	-	۴۵	**FTA_TAH.۱.۱**	در صورت برقراری نشست به طور موفقیت آمیز، محصول قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس [**روز و زمان، [هیچ مشخصه دیگری]**] باشد.
FTA_TSE.۱	-	۴۶	**FTA_TSE.۱.۱**	توابع امنیتی هدف ارزیابی باید بتواند از برقراری نشست براساس [**مکان، شماره پورت، تعداد تلاش های ناموفق احرازهویت، شناسه کاربر(نقش کاربر یا هر مشخصه امنیتی دیگر با کاربران تعریف شده)، محدوده زمانی، محدوده IP [هیچ مشخصه دیگری]**] ممانعت نماید.

۵-۱-۹- کلاس کانال‌ها و مسیرهای مورد اعتماد

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP_TRP.۱	افتا	۴۷	**FTP_TRP.۱.۱**	محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [**TLS ،HTTPS**] مسیر ارتباطی امنی فراهم کند 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 کند و تغییرات را تشخیص دهد.
FTP_TRP.۱	افتا	۴۸	**FTP_TRP.۱.۲**	محصول مورد ارزیابی به مدیر سیستم معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.
FTP_TRP.۱	افتا	۴۹	**FTP_TRP.۱.۳**	محصول مورد ارزیابی باید استفاده از کانال امن را برای احرازهویت اولیه مدیر سیستم و تمام فعالیت‌های راه‌دور مدیر سیستم الزامی نماید.
FTP_ITC.۱	افتا	۵۰	**FTP_ITC.۱.۱**	محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [TLS, HTTPS] میان خود و موجودیت IT معتبر، سرور ممیزی، سرور احرازهویت،[**سرور پنل پیامکی**] که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آنها را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.
FTP_ITC.۱	افتا	۵۱	**FTP_ITC.۱.۲**	محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.
FTP_ITC.۱	افتا	۵۲	**FTP_ITC.۱.۳**	محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [**ارسال پیامک، احرازهویت کاربر**] راه‌اندازی نماید.

۵-۱-۱۰- پیوست دو: الزامات مبتنی بر انتخاب

۵-۱-۱۱-۱- الزامات پروتکل HTTPS

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_HTTPS_EXT.۱		۵۳	**FCS_HTTPS_EXT.۱.۱**	محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC ۲۸۱۸ اجرا کند.
FCS_HTTPS_EXT.۱		۵۴	**FCS_HTTPS_EXT.۱.۲**	محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.
FCS_HTTPS_EXT.۱		۵۵	**FCS_HTTPS_EXT.۱.۳**	درصورتیکه گواهی‌نامه همتا ارائه شده، نامعتبر باشد، محصول مورد ارزیابی باید [برای برقراری اتصال درخواست مجوز نماید.]

۵-۱-۱۱-۲- الزامات پروتکل TLS Client

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان
FCS_TLSC_EXT.۱		۵۶	FCS_TLSC_EXT.۱.۱	محصول باید[(RFC ۵۲۴۶) TLS ۱.۲، (RFC ۴۳۴۶) TLS ۱.۱] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید:] • TLS_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۳۲۶۸ • TLS_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۳۲۶۸ [
FCS_TLSC_EXT.۱		۵۷	FCS_TLSC_EXT.۱.۲	محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC ۶۱۲۵، تأیید نماید.

FCS_TLSC_EXT.۱		۵۸	FCS_TLSC_EXT.۱.۳	محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید[ارتباط را برقرار نسازد،**[هیچ اقدام دیگری]**.]

۵-۱-۱۱-۳- الزامات پروتکل TLS Serve

مؤلفه	وابستگی‌ها	شماره	المان	شرح المان

FCS_TLSS_EXT.۱		۵۹	FCS_TLSS_EXT.۱.۱	محصول باید [TLS ۱.۲ (RFC۵۲۴۶)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: [• TLS_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۳۲۶۸ • TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۴۴۹۲ • TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۴۴۹۲ • TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_ SHA۲۵۶ مطابق با RFC ۵۲۴۶ • TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_ SHA۲۵۶ مطابق با RFC ۵۲۴۶ • TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶ مطابق با RFC ۵۲۸۹ • TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA۳۸۴ مطابق با RFC ۵۲۸۹ • TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ • TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹ •] ○ TLS۱۳_CHACHA۲۰_POLY۱۳۰۵_SHA۲۵۶ مطابق با RFC ۸۴۴۶ ○ TLS۱۳_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۸۴۴۶ ○ TLS۱۳_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۸۴۴۶ •]]
FCS_TLSS_EXT.۱		۶۰	FCS_TLSS_EXT.۱.۲	محصول باید اتصال‌های کاربرانی را که درخواست SSL۱.۰، SSL۲.۰، SSL۳.۰، TLS۱.۰ و [هیچ‌کدام] دارند، رد نماید.
FCS_TLSS_EXT.۱		۶۱	FCS_TLSS_EXT.۱.۳	محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [هیچ اندازه دیگری] و منحنی‌های NIST [secp۲۵۶r۱, secp۳۸۴r۱ و هیچ منحنی دیگری ،[۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید.

۵-۱-۱۱-۵- الزامات شناسایی و احرازهویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان

FIA_X۵۰۹_EXT.۱/Rev	افتا	۶۲	FIA_X۵۰۹_EXT.۱.۱	محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند: • تأیید گواهی‌نامه RFC ۵۲۸۰ و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند. • مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد. • محصول مورد ارزیابی باید برای تأیید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است • محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [هیچ روش فسخ] تأیید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند: ○ گواهی‌نامه‌های مورداستفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing » (id-kp ۳ با OID ۱.۳.۶.۱.۵.۵.۷.۳.۳) را در فیلد extendedKeyUsage خود داشته باشند ○ گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp۱ با OID ۱.۳.۶.۱.۵.۵.۷.۳.۱) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف Client "Authentication" (id-kp۱ با OID ۱.۳.۶.۱.۵.۵.۷.۳.۲) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف « OCSP Signing» (id-kp۹ با OID ۱.۳.۶.۱.۵.۵.۷.۳.۹) را در فیلد extendedKeyUsage خود داشته باشند.
FIA_X۵۰۹_EXT.۱/Rev	افتا	۶۳	FIA_X۵۰۹_EXT.۱.۲	محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.
FIA_X۵۰۹_EXT.۲	افتا	۶۴	FIA_X۵۰۹_EXT.۲.۱	محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای[TLS] و [هیچ کاربرد دیگر] **هیچ کاربرد دیگر]** از گواهی‌نامه‌های X.۵۰۹v۳ تعریف‌شده در RFC ۵۲۸۰ استفاده کند.

FIA_X۵۰۹_EXT.۲	افتا	۶۵	FIA_X۵۰۹_EXT.۲.۲	در صورتی هدف امنیتی ارزیابی قادر به برقراری ارتباط جهت تعیین اعتبار گواهی دیجیتال نباشد، توابع امنیتی هدف ارزیابی باید[گواهی را بپذیرد].

۵-۲- الزامات تضمین امنیتی

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL۱ آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام مؤلفه	توضیحات
Development	**ADV_FSP.۱**	مشخصات کارکرد ابتدایی
Guidance Documents	**AGD_OPE.۱**	راهنمای کاربری
	AGD_PRE.۱	راهنمای آماده‌سازی
Security Target	**ASE_CCL.۱**	ادعاهای انطباق
	ASE_ECD.۱	تعریف مؤلفه‌های توسعه‌یافته
	ASE_INT.۱	معرفی هدف امنیتی
	ASE_OBJ.۱	اهداف امنیتی
	ASE_REQ.۱	الزامات امنیتی معین
	ASE_TSS.۱	خلاصه مشخصات هدف ارزیابی
Tests	**ATE_IND.۱**	آزمون مستقل-منطبق
Vulnerability Assessment	**AVA_VAN.۱**	تحلیل آسیب‌پذیری
Life cycle Support	**ALC_CMC.۱**	برچسب گذاری هدف ارزیابی
	ALC_CMS.۱	پوشش پیکربندی هدف ارزیابی