به نام خدا

سند هدف امنیتی
سیستم جامع نمادایران
تحت وب
نسخه ۶.۴.۲

شرکت نمادایران

تیر۱۴۰۳

نسخه ۱.۵

فهرست

خواهشمند است در هنگام تدوین سند عبارات مشخص شده با [ ] تکمیل نموده و کروشه را حذف نمائید.

۱- معرفی سند هدف امنیتی

۱-۱- مرجع سند هدف امنیتی

عنوان سند هدف امنیتی	سیستم جامع نمادایران تحت وب
نسخه	۵
تاریخ	۱۴۰۳/۱
نویسندگان	شرکت نماد ایران

۱-۲- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	شرکت نماد ایران
نام محصول	سیستم جامع مالی و اداری تحت وب
نوع محصول	سیستم کاربردی تحت وب
نسخه	۶.۴.۲

۱-۳- مرور کلی هدف ارزیابی

۱-۳-۱- توابع امنیتی اصلی هدف ارزیابی

- ممیزی امنیت
- پشیبانی از رمزنگاری
- حفاظت از داده کاربردی
- شناسایی و احراز هویت
- مدیریت امنیت
- حفاظت از توابع امنیتی محصول
- تخصیص منابع
- دسترسی به محصول
- کانال های/مسیر مورد اعتماد

۲-۳-۱- نوع هدف ارزیابی

سیستم جامع نماد ایران تحت وب ، منطبق با پروفایل حفاظتی برنامه های کاربردی تحت شبکه می باشد.

۳-۳-۱- نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی

در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای کارکرد محصول بیان شده است:

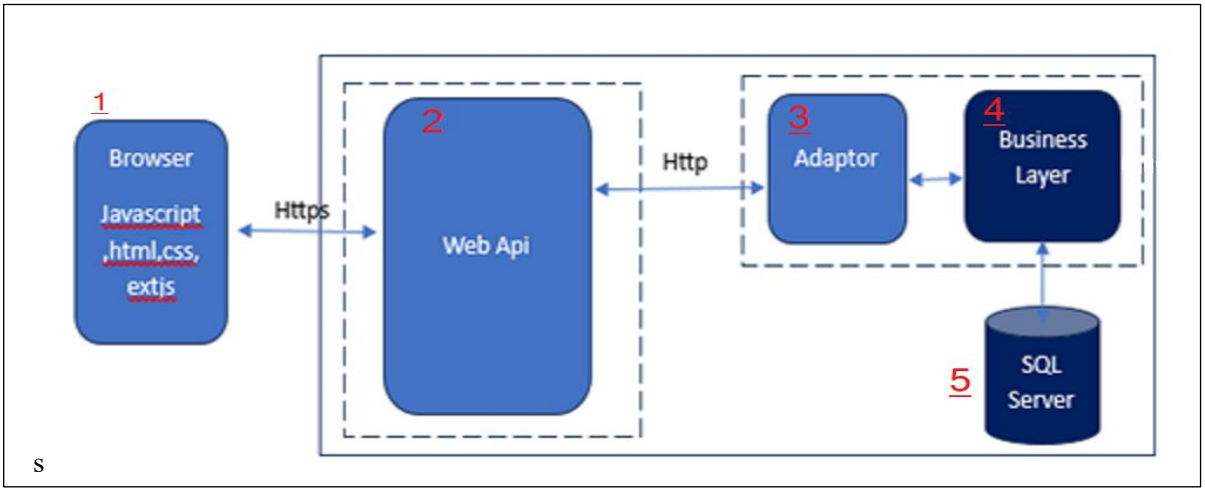
کامپوننت‌ها	حداقل الزامات
سیستم عامل	Windows Server ۲۰۱۹ or Higher
پایگاه داده	Microsoft SQL Server ۲۰۱۹ or Higher
RAM	۱۶ GB or Higher
HDD	۵۰ GB or Higher
Network	۱۰۰Mbps
.NET	.NET۶,۰

۴-۱- توصیف هدف ارزیابی

۴-۱-۱- حوزه فیزیکی

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

عناصر محصول	شماره مدل یا نسخه
پایگاه داده	Microsoft SQL Server ۲۰۱۹ or Higher
وب سرور	Microsoft Internet Information Services
ارائه دهنده سرویس پیامکی	برای احراز هویت دو عامله



توضیحات:

۱. اطلاعات کاربر از طریق مرورگر با استفاده از پروتکل HTTPS به سمت سرور ارسال می‌شود.
۲. در این مرحله، اطلاعات کاربری پردازش می‌شوند و برای ذخیره‌سازی، تحلیل، یا تغییر آن‌ها آماده می‌شوند. این اطلاعات سپس از لایه ۳ دریافت و توسط یک سرویس به نام «آداپتور» با استفاده از پروتکل HTTP فرستاده می‌شوند.
۳. اطلاعات آماده شده که توسط سرویس Web API (لایه ۳) ارسال شده‌اند، دریافت و به لایه ۴ انتقال داده می‌شوند.
٤. در این مرحله، اطلاعات دریافت شده از لایه ۳، با استفاده از منطق کسب‌وکار (Business Logic) که در این لایه پیاده‌سازی شده است، از قسمت ۵ ذخیره یا بازخوانی می‌شوند.
٥. در این لایه از Microsoft SQL Server استفاده شده تا اطلاعات در این محصول ذخیره شوند.

۲-٤-۱- 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	بوسیله نام کاربری و رمز عبور و احراز هویت دوعامله انجام می‌شود.
مدیریت امنیت	بوسیله برنامه مجوزدهی به هر کاربر یا گروه کاربری انجام می‌شود.
ممیزی	ثبت ممیزی موارد ذکر شده در الزامات امنیتی و همچنین عملیات مهم کاربران در سطح هر سیستم اطلاعاتی شرکت نماد ایران
درهم سازی/رمز نمودن داده	داده های حساس کاربر طبق الزامات و الگوریتم های ذکر شده امنیتی بصورت محرمانه نگهداری میشوند.
کانالها/مسیرهای مورد اعتماد	مسیر ارتباطی امن بین کاربران و پایگاه داده با استفاده از پروتکل HTTPS و API ها انجام می‌شود.
کنترل دسترسی	محصول قابلیت‌های لازم برای محدود کردن دسترسی را دارد، به طوری که تنها موجودیت‌های مجاز به داده و کارکردهای محصول دسترسی دارند.
کنترل گردش مستندات و اطلاعات	حداکثر اندازه فایل میتواند به صورت پویا برای هر نوع سند تعریف شود.همچنین تنها کاربران مجاز،مجوز صدور و ارسال هر رکورد را دارند.
حفاظت از داده ها	محصول به هیچگونه منبعی (نرم افزاری و سخت افزاری) دسترسی ندارد و تنها با ارتباط امن به شبکه متصل می‌شود.
حفاظت از محصول	محصول تنها از امکانات امنیتی که در پلتفرم (ویندوز و .Net)ارائه شده است بهره میبرد، مانند مدیریت حافظه و استفاده از API های ارائه شده توسط آنها.

کارکردها	توصیف
به روزرسانی امن	بروز رسانی امن به صورت دستی انجام می‌شود. DLL ها بوسیله امضاء دیجیتال محافظت می‌شوند.

۲- ادعای انطباق

۲-۱- انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استلندارد ارزیابی امنیتی معیار مشترک	IRISI/ISO ۱۵٤۰۸ V۳,۱R٤
انطباق با SFRها (قسمت دوم از CC)	توسعه یافته
انطباق با SARها (قسمت سوم از CC)	منطبق

۲-۲- انطباق با پروفایل حفاظتی

نام پروفایل حفاظتی	برنامه های کاربردی تحت شبکه (اسفند ۹۶ نسخه ۱.۱)

۲-۳- انطباق با سطح تضمین امنیتی

سطح تضمین امنیتی	EAL ۱

۳- تعریف مسائل امنیتی

۳-۱- خطمشی

خطمشی	توصیف
ممیزی کامل	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.
پیکربندی مناسب	پیکربندی پیش‌فرض محصول و مولفه¬های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و

خطمشی	توصیف
	محیط عملیاتی آن به دست آورد. سرویس هایی 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، پورت¬های پیش‌فرض، صفحات پیش‌فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می¬نمایند. این خط مشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه 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.
امضای دیجیتال	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۲-۳- تهدیدات

تهدید	توصیف
دسترسی غیرمجاز	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.
تغییر غیرمجاز	رکوردهای، مستندات و داده¬های حفاظت شده توسط محصول می¬تواند بدون مجوز تغییر یابند. مهاجم می-تواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می¬تواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده¬های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می¬دهد که صحت رکوردها و مستندات تضمین شده نمی¬باشد. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد

تهدید	توصیف
	منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.
انکار	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول می¬تولند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول می¬باشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می¬تولند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم می¬تواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.
افشای اطلاعات	داده¬های محرمانه که توسط محصول محافظت می¬شوند می¬تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می¬تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی می¬تولند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده می¬تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	مهاجم می¬تواند سبب گردد محصول در یک بازه زمانی غیر قابل دسترسی یا بلا استفاده گردد. این امر معمولاً با ارسال درخواست¬های بسیار در یک بازه زمانی کوتاه صورت می¬گیرد طوریکه محصول قادر به پاسخ نخواهد بود. نوع ساده¬ای از حمله شامل ارسال درخواست¬های بسیار از یک رنج IP مشخص می باشد که به نام حمله DoS شناخته می¬شود. نوع دیگر پیشرفته¬تر حمله DDoS می¬باشد که از BOTNET استفاده می¬نماید و محدودیتی بر روی آدرس IP ورودی ندارد.
داده های ورودی مخرب	مهاجم میتواند یک رکورد، سند یا داده مضر را در داخل محصول وارد کند. با استفاده از این تهدید، مهاجم میتواند به داده کاربر خاص دسترسی پیدا کند، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
سطح دسترسی بالاتر	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.
شنود شبکه	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 می نماید.

۳-۳- فرضیات

فرضیه	توصیف
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
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 می‌نمایند.
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 آسیب‌پذیری‌های شناخته شده را اتخاذ می‌نمایند.
محیط امن	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 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.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره‌سازی 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.
ارتباطات	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.
تحویل امن	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.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.

٤- اهداف امنیتی

٤-١- اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
ممیزی	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.
احراز هویت	محصـــول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصـــول 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 بنـدی آنهـا قوانینی را تعریف نمـایـد. همچنین برای مســـتنـدات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم می‌نماید. محصـــول باید برای کاربران به صـــورت 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.
کنترل جریان داده	محصـــول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواســت‌ها از یک رنج IP تعریف شـده می‌تواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیسـتم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شـــبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.

هدف امنیتی	توصیف
صحت داده	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.
مدیریت	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.
مدیریت خطا	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 برگردلند، 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.
مدیریت داده‌های باقیمانده	محصول باید اطمینان دهد که هر داده‌ی باقیمانده از محصول زمانیکه دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس می‌گردد.
ارتباطات امن مبتنی برTLS	تمام کلنال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

۲-٤- اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توصیف
محیط امن	محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. 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 محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله

هدف امنیتی	توصیف
	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 دهنده‌ی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله-ای 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 مولفه‌های 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 تست باید پاک یا غیر قابل دسترس گردند.
پشتیبان‌گیری مناسب	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده‌های باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روال‌های از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مولفه‌های سخت-افزاری نیز نسخه پشتیبان تهیه گردد.

۵- نیازمندی‌های امنیتی

۵-۱- الزامات کارکرد امنیتی

الزامات کارکردامنیتی زیر مطابق پروفایل حفاظتی برنامه های کاربردی تحت شبکه تهیه شده‌اند

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۱	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
٤		بازبینی داده ممیزی ۱	FAU_SAR.۱،۱
٥		بازبینی داده ممیزی ۲	FAU_SAR.۱.۲
٦		بازبینی داده ممیزی محدود۱	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		ذخیره سازی رویدادهای ممیزی ۱	FAU_STG.۱،۱
۱۰		ذخیره سازی 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.٤،۱
۱۳	کلاس پشتیبانی از رمزنگاری	عملیات رمزنگاری ۱ (۱)	FCS_COP.۱،۱(۱)
۱٤		عملیات رمزنگاری ۱ (۲)	FCS_COP.۱،۱(۲)
۱٥		الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.۱،۱
۱٦		الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.۱،۲
۱۷		الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.۱،۳
۱۸		الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.۱،٤

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۱۹		خط مشی کنترل دسترسی ۱	FDP_ACC.۱،۱
۲۰		عملیات کنترل دسترسی ۱	FDP_ACF.۱،۱
۲۱		عملیات کنترل دسترسی ۲	FDP_ACF.۱،۲
۲۲		عملیات کنترل دسترسی ۳	FDP_ACF.۱،۳
۲۳		عملیات کنترل دسترسی ۴	FDP_ACF.۱،٤
۲٤		حفاظت کامل از اطلاعات باقیمانده در منابع	FDP_RIP.۲،۱
۲٥		ورود داده کاربری به محصول با مشخصه امنیتی ۱	FDP_ITC.۲،۱
۲٦		ورود داده کاربری به محصول با مشخصه امنیتی۲	FDP_ITC.۲،۲
۲۷		ورود داده کاربری به محصول با مشخصه امنیتی ۳	FDP_ITC.۲،۳
۲۸		ورود داده کاربری به محصول با مشخصه امنیتی ۴	FDP_ITC.۲،٤
۲۹	**حفاظت از داده کاربر**	ورود داده کاربری به محصول با مشخصه امنیتی ۵	FDP_ITC.۲،٥
۳۰		خروج داده کاربری از محصول با مشخصه امنیتی ۱	FDP_ETC.۲،۱
۳۱		خروج داده کاربری از محصول با مشخصه امنیتی ۲	FDP_ETC.۲،۲
۳۲		خروج داده کاربری از محصول با مشخصه امنیتی ۳	FDP_ETC.۲،۳
۳۳		خروج داده کاربری از محصول با مشخصه امنیتی ۴	FDP_ETC.۲،٤
۳٤		صحت داده کاربری ذخیره شده۲	FDP_SDI.۲،۱
۳٥		صحت داده کاربری ذخیره شده۳	FDP_SDI.۲،۲
۳٦		مدیریت احرازهویت ناموفق۱	FIA_AFL.۱،۱
۳۷		مدیریت احرازهویت ناموفق۲	FIA_AFL.۱،۲
۳۸		تعریف مشخصات کاربر۱	FIA_ATD.۱،۱

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۳۹	شناسایی و احراز هویت	مدیریت کلمه عبور	FIA_PMG_EXT.۱،۱
٤۰		احرازهویت کاربر۱	FIA_UID.۲،۱
٤۱		احرازهویت کاربر۲	FIA_UID.۱،۲
٤۲		احراز هویت قبل از هر اقدام ۱	FIA_UAU.۲،۱
٤۳		سازوکار احرازهویت چندگانه۱	FIA_UAU.۵،۱
٤٤		سازوکار احرازهویت چندگانه۲	FIA_UAU.۵،۲
٤۵		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر۱	FIA_USB.۱،۱
٤٦		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.۱،۲
٤۷		انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر۳	FIA_USB.۱،۳
٤۸		الزامات پروتکل X۵۰۹ (۱)/ ابطال	FIA_X۵۰۹_EXT.۱،۱/Rev
٤۹		الزامات پروتکل X۵۰۹ (۲)/ ابطال	FIA_X۵۰۹_EXT.۱،۲/Rev
۵۰		الزامات پروتکل X۵۰۹ (۱)	FIA_X۵۰۹_EXT.۲،۱
۵۱		الزامات پروتکل X۵۰۹ (۲)	FIA_X۵۰۹_EXT.۲،۲
۵۲	مدیریت امنیت	مدیریت کارکرد در محصول۱	FMT_MOF.۱،۱
۵۳		مدیریت مشخصه های امنیتی۱	FMT_MSA.۱،۱
۵٤		مدیریت مشخصه های امنیتی ۳	FMT_MSA.۳،۱
۵۵		مدیریت مشخصه های امنیتی ۴	FMT_MSA.۳،۲
۵٦		مدیریت داده‌های محصول ۱ – مدیر سیستم	FMT_MTD.۱،۱ (۱)
۵۷		مدیریت داده‌های محصول ۱ – کاربر عادی، وارد کننده داده	FMT_MTD.۱،۱ (۲)
۵۸		کارکردهای مدیریتی محصول۱	FMT_SMF.۱،۱
۵۹		نقشهای امنیتی ۱	FMT_SMR.۱،۱
٦۰		نقشهای امنیتی ۲	FMT_SMR.۱،۲
٦۱		حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.۱،۱

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
٦٢	**حفاظت از داده توابع امنیتی هدف ارزیابی**	انتقال داده امنیتی در داخل محصول۱	FPT_ITT.۱،۱
٦٣		سازگاری داده امنیتی بین محصول و موجودیت امن۱	FPT_TDC.۱،۱
٦٤		مهرهای زمانی۱	FPT_STM.۱،۱
٦٥		به روزرسانی امن۲	FPT_TUD_EXT.۱،۲
٦٦		به روزرسانی امن۳	FPT_TUD_EXT.۱،۳
٦٧	**تخصیص منابع**	تحمل خطا۱	FRU_FLT.۱،۱
٦٨	**دسترسی به محصول**	محدودیت بر روی چندین نشست همزمان ۱	FTA_MCS.۱،۱
٦٩		محدودیت بر روی چندین نشست همزمان ۲	FTA_MCS.۱،۲
٧٠		خاتمه دادن به نشستها توسط محصول۱	FTA_SSL.۳،۱
٧١		خاتمه دادن به نشستها توسط کاربر۱	FTA_SSL.٤،۱
٧٢		سوابق دسترسی به محصول۱	FTA_TAH.۱،۱
٧٣		سوابق دسترسی به محصول۲	FTA_TAH.۱،۲
٧٤		سوابق دسترسی به محصول۳	FTA_TAH.۱،۳
٧٥		برقراری نشست۱	FTA_TSE.۱،۱
٧٦	**کانال‌ها و مسیرهای امن**	مسیر امن ۱	FTP_TRP.۱،۱
٧٧		مسیر امن ۲	FTP_TRP.۱،۲
٧٨		مسیر امن ۳	FTP_TRP.۱،۳
٧٩		کانال امن ۱	FTP_ITC.۱،۱
٨٠		کانال امن ۲	FTP_ITC.۱،۲
٨١		کانال امن ۳	FTP_ITC.۱،۳
٨٢	**عملیات رمزنگاری**	الزامات پروتکل TLS Client(۱)	FCS_TLSC_EXT.۱،۱
٨٣		الزامات پروتکل TLS Client(۲)	FCS_TLSC_EXT.۱،۲
٨٤		الزامات پروتکل TLS Client(۳)	FCS_TLSC_EXT.۱،۳

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۸۵		الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.۱،٤
۸٦		الزامات پروتکل TLS Server (۱)	FCS_TLSS_EXT.۱،۱
۸۷		الزامات پروتکل TLS Server (۲)	FCS_TLSS_EXT.۱،۲
۸۸		الزامات پروتکل TLS Server (۳)	FCS_TLSS_EXT.۱،۳
۸۹		الزامات پروتکل TLS Server/ احرازهویت (۴)	FCS_TLSS_EXT.۲،٤
۹۰		الزامات پروتکل TLS Server/ احرازهویت (۵)	FCS_TLSS_EXT.۲،٥
۹۱		الزامات پروتکل TLS Server/ احرازهویت (۶)	FCS_TLSS_EXT.۲،٦

۲-۵- کلاس ممیزی امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_GEN.۱	- FPT_STM.۱	۱	FAU_GEN.۱،۱	محصول بر اساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید میکند: • آغاز و اتمام توابع ممیزی • تمامی رویدادهای قابل ممیزی (برای نوع داده حساس و داده هایی که بار حقوقی دارند) که در جدول یک آمده است.
		۱	FAU_GEN.۱،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 • **[هر نوع اطلاعات قابل ممیزی دیگر از قبیل آدرس IP کاربرو نام کاربری، زمان و تاریخ انجام فعالیت]**
FAU_GEN.۲	- FAU_GEN.۱ - FIA_UID.۱	۲	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	- FAU_GEN.۱	۳	FAU_SAR.۱،۱	محصول باید امکان خواندن [**کلیه‌ی رویدادهای ممیزی**]از کل رکوردهای ممیزی را برای[**کاربران یا گروه‌های کاربری مجاز]** فراهم نماید.
		٤	FAU_SAR.۱،۲	باید رکوردهای ممیزی را طوری فراهم نماید که کاربر بتواند آن‌ها را درک و اطلاعات این رکوردها را تفسیر نماید.
FAU_SAR.۲	- FAU_SAR.۱	٥	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.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FAU_SAR.۳	- FAU_SAR.۱	٦	FAU_SAR.۳،۱	محصول باید امکان انجام**[متدهای انتخاب و مرتب سازی]** رکوردهای ممیزی را به نحوی فراهم کند که کاربر مجاز بتواند آن رکوردها را براساس **[حساب کاربری، تاریخ/زمان، مکان، روش اتصال کاربر، درجه اهمیت رکوردها، نوع رخداد و هیچ پارامتر مورد نیاز دیگری]**مرتب کند.
FAU_SEL.۱	- FAU_GEN.۱ - FMT_MTD.۱	۷	FAU_SEL.۱،۱	محصول باید قادر باشد براساس مشخصه‌های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادها را جهت ممیزی شدن، انتخاب نماید: • [نوع رخداد] • **[تنها رخدادهای ممیزی کم‌اهمیت باید برای عدم ثبت در فایل‌های ممیزی انتخاب شوند]**
FAU_STG.۱	- FAU_GEN.۱	۸	FAU_STG.۱،۱	محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره سازی را، از حذف غیرمجاز حفاظت نماید.
		۹	FAU_STG.۱،۲	محصول باید قادر به [تشخیص] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره سازی آنها باشد**.**
FAU_STG.۳	- FAU_STG.۱	۱۰	FAU_STG.۳،۱	محصول در صورت تجاوز دنباله ممیزی از [یک **محدودیت از پیش تعریف شده]** باید **[با استفاده از ایمیل یا پیام کوتاه،یک پیغام در گردش کار،از طریق واسطهای محصول کاربران مربوطه را مطلع میکند.]**
FAU_STG.۴	- FAU_STG.۱	۱۱	FAU_STG.٤،۱	محصول در صورت پر شدن دنباله ممیزی، باید [رویدادهای ممیزی را نادیده بگیرد] و[به **تعداد x رکورد(طبق تنظیم تعداد رکورد حذف از لاگ) از ابتدای جدول لاگ،رکوردها را حذف میکند.]**

جدول یک - لیست رویدادهای قابل ممیزی

مؤلفه	رویداد قابل ممیزی	جزئیات
مرتبط نمودن هویت کاربر به رویداد۱	تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
بازبینی داده ممیزی۱	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
انتخاب داده ممیزی۱	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 ممیزی۱	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)	
صحت داده های کاربری ذخیره شده ۲	تلاشهای موفقیت آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاشها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)	
احراز هویت کاربر	ثبت کاربرد ناموفق از سازوکار احرازهویت (حداقل) ثبت تمام کاربردهای سازوکار احراز هویت (پایه)	
سازوکار احرازهویت چندگانه	ثبت نتایج احرازهویت (حداقل) ثبت هر سازوکاراحرازهویت فعال همراه با نتیجه نهائی(پایه)	

مؤلفه	رویداد قابل ممیزی	جزئیات
شناسایی کاربر	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبدأ، شناسایی نقطه پایانی اتصال
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)	برای مثال، رد و یا قبول کلمه عبور کاربر
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- مدیرسیستم	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 رکوردهاواسناد باید ثبت شود.
عملیات رمزنگاری(۲)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه های موجودیتهای فعال و غیرفعال (پایه)	
عملیات کنترل دسترسی	درخواستهای موفقیت آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل) تمامی درخواستهای (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	
ورود داده های کاربری به محصول با مشخصه امنیتی	ورود داده کاربری موفقیت آمیز، شامل هرگونه مشخصه های امنیتی (حداقل) تمامی تلاشها برای وارد کردن داده های کاربری، شامل هرگونه مشخصه های امنیتی (پایه)	شناسایی داده های موجودیت غیرفعال

مؤلفه	رویداد قابل ممیزی	جزئیات
خروج داده های کاربری از محصول با مشخصه امنیتی	خروج اطلاعات به‌طور موفقیت آمیز (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 است (حداقل)	
سازگاری داده های امنیتی بین محصول و موجودیت امن	ثبت استفاده موفق از سازوکار سازگاری داده های محصول (حداقل) ثبت استفاده از سازوکار سازگاری داده های 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 است (پایه)	
برقراری نشست	ثبت منع آغاز نشست به دلیل سازوکار آغاز نشست (حداقل) ثبت تمامی تلاشها در آغاز نشست کاربر (پایه)	
محدودیت بر روی چندین نشست همزمان	ثبت رد یک نشست مبتنی بر محدودیت نشستهای همزمان (حداقل)	

مؤلفه	رویداد قابل ممیزی	جزئیات
خاتمه دادن به نشستها	ثبت خاتمه دادن به یک نشست بیکار توسط سازوکار قفل نشست (حداقل) ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)	

۳-۵- کلاس پشتیبانی از رمزنگاری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FCS_COP.۱(۱)	- FDP_ITC.۱ - FDP_ITC.۲ - FCS_CKM.۱	۱	**FCS_COP.۱،۱(۱)**	محصـول باید[**برای وارسـی صـحت داده‌های ممیزی و داده‌های رکورد]** بر اسـاس یک الگوریتم رمزنگاری مشـخص[**SHA-۲۵۶**]واندازه کلید رمزنگاری [**هیچکدام]** اجرا شـود که مطابق با **FIPS** [۱۸۰-۲]باشد.
FCS_COP.۱(۲)	- FDP_ITC.۱ - FDP_ITC.۲ - FCS_CKM.۱	۲	**FCS_COP.۱،۱(۲)**	*محصول باید* **برای[تولید داده درهم سازی]***بر اساس مجموعه الگوریتم‌های رمزنگاری مشخص* **SHA-۲۵۶**و اندازه‌کلید رمزنگاری **۲۵۶** *اجرا شود که مطابق با* **FIPS** ۱۸۰-۲ *باشد*.
	-	۳	**FCS_TLSC_EXT.۱.۱**	محصول باید[TLS ۱،۲ (RFC۵۲۴۶)]را پیاده سازی کند و دیگر نسخه های TLSو SSLرا رد کند. همچنین TLSرا با پشتیبانی از مجموعه های رمز زیر را پیاده سازی کند: o TLS_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۳۲۶۸ o TLS_RSA_WITH_AES_۱۹۲_CBC_SHA مطابق با RFC ۳۲۶۸ o TLS_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۳۲۶۸ o TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۳۲۶۸ o TLS_DHE_RSA_WITH_AES_۱۹۲_CBC_SHA مطابق با RFC ۳۲۶۸ o TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ۳۲۶۸ o TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ٤٤۹۲ o TLS_ECDHE_RSA_WITH_AES_۱۹۲_CBC_SHA مطابق با RFC ٤٤۹۲ o TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA مطابق با RFC ٤٤۹۲

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA مطابق با ٤٤٩٢ RFC
				○ TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_CBC_SHA مطابق با ٤٤٩٢ RFC
				○ TLS_ECDHE_ECDSA_WITH_AES_۲٥٦_CBC_SHA مطابق با ٤٤٩٢ RFC
				○ TLS_RSA_WITH_AES_۱۲۸_CBC_SHA۲٥٦ مطابق با ٥٢٤٦ RFC
				○ TLS_RSA_WITH_AES_۱۹۲_CBC_SHA۲٥٦ مطابق با ٥٢٤٦ RFC
				○ TLS_RSA_WITH_AES_۲٥٦_CBC_SHA۲٥٦ مطابق با ٥٢٤٦ RFC
				○ TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_ SHA۲٥٦ مطابق با ٥٢٤٦ RFC
				○ TLS_DHE_RSA_WITH_AES_۱۹۲_CBC_ SHA۲٥٦ مطابق با ٥٢٤٦ RFC
				○ TLS_DHE_RSA_WITH_AES_۲٥٦_CBC_ SHA۲٥٦ مطابق با ٥٢٤٦ RFC
				○ TLS _RSA_WITH_AES_۱۲۸_GCM_ SHA۲٥٦ مطابق با ٥٢٨٨ RFC
				○ TLS _RSA_WITH_AES_۱۹۲_GCM_ SHA۲٥٦ مطابق با ٥٢٨٨ RFC
				○ TLS _RSA_WITH_AES_۲٥٦_GCM_ SHA۳۸٤ مطابق با ٥٢٨٨ RFC
				○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA۲٥٦ مطابق با ٥٢٨٩ RFC
				○ TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_CBC_SHA۲٥٦ مطابق با ٥٢٨٩ RFC
				○ TLS_ECDHE_ECDSA_WITH_AES_۲٥٦_CBC_SHA۳۸٤ مطابق با ٥٢٨٩ RFC
				○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲٥٦ مطابق با ٥٢٨٩ RFC
				○ TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_GCM_SHA۲٥٦ مطابق با ٥٢٨٩ RFC
				○ TLS_ECDHE_ECDSA_WITH_AES_۲٥٦_GCM_SHA۳۸٤ مطابق با ٥٢٨٩ RFC
				○ TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲٥٦ مطابق با ٥٢٨٩ RFC
				○ TLS_ECDHE_RSA_WITH_AES_۱۹۲_GCM_SHA۲٥٦ مطابق با ٥٢٨٩ RFC

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸٤ مطابق با RFC ۵۲۸۹ ○ TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵٦ مطابق با RFC ۵۲۸۹ ○ TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵٦ مطابق با RFC ۵۲۸۹ ○ TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA۳۸٤ مطابق با RFC ۵۲۸۹].
	-	٤	**FCS_TLSC_EXT.** ۱،۲	محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶از RFC ٦۱۲۵ تائید کند.
	-	٥	**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**]]
FCS_TLSC_EXT.۱،٤	-	٦	FCS_TLSC_EXT.۱. ٤	محصول باید [Supported Elliptic Curves Extension]را به همراه NIST curve های [secp۲۵٦r۱, secp۳۸٤r۱, secp۵۲۱r۱ و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.
FCS_HTTPS_EXT.۱،۱	-	۷	FCS_HTTPS_EXT. ۱،۱	• محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC ۲۸۱۸ اجرا کنند.
FCS_HTTPS_EXT.۱،۲	-	۸	FCS_HTTPS_EXT. ۱،۲	محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.
FCS_HTTPS_EXT.۱،۳	-	۹	FCS_HTTPS_EXT. ۱،۳	درصورتی‌که گواهی‌نامه همتا ارائه شده، نامعتبر باشد، محصول مورد ارزیابی باید [اتصال را برقرار ننماید، برای برقراری اتصال درخواست مجوز نماید، هیچ اقدام دیگری انجام ندهد.]

٤-٥- کلاس شناسایی و احرازهویت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_AFL.۱	FIA_UAU.۱ -	۱	FIA_AFL.۱،۱	محصول باید بتواند با استفاده از یک عدد مثبت قابل تنظیم توسط مدیر[**بازه‌ی ۱ الی ۱ بیشتر**] ، تلاش‌های ناموفق احرازهویت مرتبط با[لیستی از رویدادهای احرازهویت]را تشخیص دهد.
		۲	FIA_AFL.۱،۲	زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [به حد تعیین شده رسید، بیشتر از حد تعیین شده رسید،]محصول باید [**غیر فعال شدن حساب کاربری**] را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود
FIA_ATD.۱	- -	۳	FIA_ATD.۱،۱	محصول باید مشخصه های امنیتی زیر را برای هر کاربر نگهداری نماید: [• **شناسه کاربر** • **متد احرازهویت مورد استفاده** • **داده احرازهویت** • **نقش کاربر** • **وضعیت حساب کاربری(فعال، غیرفعال، بلوکه شده و غیره)** • **[هیچ مشخصه امنیتی دیگر]]**
	-	٤	FIA_PMG_EXT.۱،۱	محصول باید قابلیتهای مدیریت کلمه عبور را که در زیر ذکر شده لند برای کلمه های عبور مدیریتی فراهم کند: ۱. کلمه عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص مانند**[" @ "**]،**["هیچ کاراکتر دیگری"**]]باشد.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				۲. حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم میباشد و ۸ کاراکتر یا بیشتر باشد.
FIA_UAU.۲	- FIA_UID.۲	۵	FIA_UID.۲،۱	توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت شناسایی نماید.
	-	٦	FIA_UAU.۲،۱	توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت احراز هویت نمایند
FIA_UAU.۵	- -	۷	FIA_UAU.۵،۱	محصول باید به منظور احرازهویت کاربر سازوکارهای زیر را فراهم آورد: **]** • **نام کاربری و کلمه عبور** • **احراز هویت چندگانه با استفاده از پیامک]**
		۸	FIA_UAU.۵،۲	محصول باید هر کاربر متقاضی احرازهویت را مطابق قوانین ذیل احرازهویت نماید: **[کاربران از راه‌دوربلید علاوه بر بررســی‌نام کاربری و کلمه عبور از روش احرازهویت چندگانه (مانند Dual factor authentication) استفاده کند.** **[OTP یا توکن و از این قبیل موارد]]**
FIA_USB.۱	- FIA_ATD.۱	۹	FIA_USB.۱،۱	محصول باید مشخصه های امنیتی زیر را برای کاربر فعال نگهداری کند: **]** • **شناسه کاربر** • **نقشها و یا مجموعه دسترسیهای کاربر به قسمتهای مختلف برنامه** • **جزئیات واسط کلاینت** • **پیشینه احرازهویت(جزئیات تلاش برای احرازهویت موفق و ناموفق)** • **[هیچ مشخصه کاربری دیگری]]**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
		۱۰	FIA_USB.۱،۲	محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت میکند، اعمال کند: • **[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 به روزرسانی گردد.** • **[هیچ قانون دیگری برای اتصال اولیه مشخصه ها]]**
		۱۱	FIA_USB.۱،۳	محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه های امنیتی کاربر فعال اعمال کند: [**هیچ تغییری در طول نشست فعال مجاز نیست** **[هیچ قوانین دیگری حاکم بر تغییرات مشخصه ها]]**
FIA_X۵۰۹_EXT.۱،۱/Rev	-	۱۲	FIA_X۵۰۹_EXT.۱،۱/Rev	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 [پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC ۶۹۶۰] تأیید کند.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• 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 ۱,۳,٦,۱,٥,٥,۷,۳,۱ OID) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف Client "Authentication” (id-kp۱ با ۱,۳,٦,۱,٥,٥,۷,۳,۲ OID) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp۹ با ۱,۳,٦,۱,٥,٥,۷,۳,۹ OID) را در فیلد extendedKeyUsage خود داشته باشند.
FIA_X٥٠٩_EXT.١,٢/Rev	-	١٣	FIA_X٥٠٩_EXT.١,٢/Rev	محصـــول مورد ارزیابی تنها درصـــورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شـده باشـد و پرچم CA به حالت «TRUE» تنظیم‌شـده باشـد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.
FIA_X٥٠٩_EXT.٢,١	-	١٤	FIA_X٥٠٩_EXT.٢,١	محصـول مورد ارزیابی باید جهت پشـتیبانی احرازهویت برای [TLS, HTTPS]، و هیچ کاربرد دیگر] از گواهی‌نامه‌های X.٥٠٩v٣ تعریف‌شده در RFC ٥٢٨٠ استفاده کند.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FIA_X۵۰۹_EXT.۲,۲	-	۱۵	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 [به مدیر سیستم این امکان را بدهد که در زمینه‌ی پذیرش گواهی تصمیم‌گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد.]

۵-۵- کلاس حفاظت از داده کاربری

مؤلفه	وابستگی ها	شماره	المان	شرح المان
	-	۱	FDP_ACC.۱،۱	محصول باید [**خط مشی های کنترل دسترسی**] را بر روی موارد زیر اعمال کند :] • **موجودیت فعال :** • **[مدیر سیستم، کاربر عادی،[هیچ موجودیت فعال دیگر]]** • **موجودیت غیرفعال:** ○ **رکوردها، مستندات و فرا-داده** **داده متعلق به کاربران** ○ **داده احرازهویت** **داده با این معیارها[هیچ معیار داده دیگر]** ○ **[هیچکدام از موجودیتهای غیرفعال دیگر]** • **عملیات:** **ایجاد موجودیت غیرفعال جدید** **حذف موجودیت غیرفعال** **تغییر دسترسیها به موجودیت غیرفعال** **عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال** **[هیچ عملیات دیگری]** **[**
	-	۲	FDP_ACF.۱،۱	محصول باید **[خط مشیهای کنترل دسترسی]**را با توجه به موارد زیر بر روی موجودیتهای غیرفعال اعمال کند:] • **هویت کاربر**

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				• **نقشها و مجوزهای کاربر مجاز** • **اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده میشوند** • **[هیچ مشخصه ای از موجودیت فعال]]**
	-	۳	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].**
	-	٤	FDP_ACF.۱،۳	محصول باید بر اساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: [• **کاربران با مجوز مدیر سیستم به رکوردهای لازمه مدیریت سیستم و نیز روش ارائه شده توسط محصول، دسترسی دارند** • **کاربران غیرمجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند.** • **[هیچ قانون دیگری]** [
	-	٥	FDP_ACF.۱،٤	محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری کند: [

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]]**
	-	٦	FDP_RIP.٢,١	محصول باید تضمین کند 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_ITC.٢,١	-	٧	FDP_ITC.٢,١	محصول باید هنگام دریافت داده کاربری، [**خط‌مشی کنترل دسترسی**] را اعمال نماید.
FDP_ITC.٢,٢	-	٨	FDP_ITC.٢,٢	محصول باید از مشخصه‌های امنیتی مرتبط با داده 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 و از این قبیل موارد.
FDP_ITC.٢,٣	-	٩	FDP_ITC.٢,٣	محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال داده، ارتباط و همبستگی شفافی را بین مشخصه‌های امنیتی و داده کاربری دریافت شده، فراهم می‌نماید.
	-	١٠	FDP_ITC.٢,٤	محصول باید اطمینان دهد که تفسیر مشخصه‌های امنیتی داده‌های کاربری دریافت شده همانند، آنچه که فرستنده داده کاربری در نظر گرفته، می‌باشد.
	-	١١	FDP_ITC.٢,٥	محصول باید هنگام ورود داده کاربری از بیرون (خارج از محصول)، قوانین تحت کنترل خط‌مشی امنیتی زیر را اعمال نماید:

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				[**قوانین کنترلی اضافی هنگام ورود داده کاربری**.]
FDP_ETC.۲.۱	-	۱۲	FDP_ETC.۲،۱	محصول باید هنگام خروج داده کاربری به بیرون[۱] [**خط‌مشی کنترل دسترسی**] را اعمال نماید.
FDP_ETC.۲.۲	-	۱۳	FDP_ETC.۲،۲	محصـــول بـاید بـه همراه داده کـاربری خروجی (انتقـال داده بـه بیرون از محصـــول)، مشخصه‌های امنیتی مرتبط با داده کاربری را نیز انتقال دهد.
	-	۱٤	FDP_ETC.۲،۳	محصـول باید اطمینان دهد که مشـخصـه‌های امنیتی در هنگام خروج داده از محصـول، ارتباط و پیوند شفافی با داده کاربری خارج شده دارند.
FDP_ETC.۲.۴	-	۱٥	FDP_ETC.۲،٤	محصول باید هنگام خروج داده کاربری به بیرون (خارج از محصول)، قوانین زیر را اعمال نماید: [**مدیر سیستم باید خروج رکوردها را محدود نماید، به طوری‌که کاربران محصول، قادر به خروج بدون هدف داده به بیرون از آن (خارج از محصول) نباشند**.]
	-	۱٦	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**] داده های رکورد و داده های ممیزی را بر اساس مشخصه های[**درهم شده داده های کاربری ذخیره شده**] پایش کند

[۱] Export user data

مؤلفه	وابستگی ها	شماره	المان	شرح المان
	-	۱۷	FDP_SDI.۲,۲	هنگام تشخیص خطای صحت داده، محصول باید **[در هنگام نمایش فرمهای دارای داده های حساس،اقدام به قرمز کردن ردیفهای دارای خطا]** را صورت دهد.

۲-۵-۵- کلاس مدیریت امنیت

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MOF.۱	- FMT_SMR.۱	۱	FMT_MOF.۱،۱	محصول باید امکان[تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] توابع [**تمام کارکردهای مربوط به مدیریت محصول**]را به[**مدیر سیستم و هر کاربری که مجوز لازم را دارد[هیچ نقش دیگری]]**،محدود کند.
FMT_MSA.۱	- FDP_ACC.۱ - FMT_SMR.۱ - FMT_SMF.۱	۲	FMT_MSA.۱،۱	محصول باید با اعمال [**خط‌مشی کنترل دسترسی]**، [امکان تغییر پیش‌فرض، پرس و جو، تغییر، حذف، [**هیچ عملیات دیگری]]** مشخصه‌های امنیتی **[نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت های مختلف برنامه]** را به [**مدیر سیستم و هر کاربری که مجوز لازم را دارد]** محدود نماید.
	-	۳	FMT_MSA.۳،۱	محصول برای مشخصه‌های امنیتی که برای اعمال **[خط مشی]** استفاده می‌شوند، باید مقادیر پیش فرض محدود شده‌ای درنظر بگیرد.
	-	٤	FMT_MSA.۳،۲	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 (۱)	- FMT_SMR.۱	٥	FMT_MTD.۱،۱ (۱)	محصول باید توانایی[پرس وجو، حذف،**[هیچ اقدام دیگر]]** [**داده های ممیزی ،حفاظت از داده کاربری و مدیریت امنیت]** را به[**مدیر سیستم و هر کاربری که مجوز لازم را دارد**]محدود نماید.

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FMT_MTD.۱ (۱)	FMT_SMR.۱ -	٦	FMT_MTD.۱،۱ (۲)	محصول باید توانایی [پرس‌وجو، تغییر، حذف، **[هیچ کارکرددیگری**]] [**تمام فرمهای سیستم های تحت وب نمادایران تحت مالکیت و دسترسی کاربر عادی]** به [**کاربر عادی]** محدود نماید.
	-	۷	FMT_SMF.۱،۱	محصول باید قادر به انجام [**کارکردهای مدیریتی که در جدول دو آمده است]** باشد
FMT_SMR.۱	FIA_UID.۱ -	۸	FMT_SMR.۱،۱	نقشهای زیر در محصول باید تعریف شده باشد: [مدیر سیستم، کاربر عادی ،[**هیچ نقش دیگر مجاز معرفی شده]]**
		۹	FMT_SMR.۱،۲	محصول، باید قادر به مرتبط نمودن کاربران با نقشها و دسترسی های مجاز تعریف شده باشند.

جدول دو - کارکردهای مدیریتی

مؤلفه	عملیات مدیریتی
بازبینی داده ممیزی۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
اقدامات لازم در زمان از دست رفتن داده ممیزی۱	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی
پیشگیری از اتلاف و از بین رفتن داده های ممیزی ۱	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی
عملیات کنترل دسترسی	مدیریت مشخصه های 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 آزادسازی) 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 شده۲	عملیاتی برای تشخیص یک خطای صحت داده که میتواند قابل پیکربندی باشد.
مدیریت احراز هویت ناموفق	مدیریت حد آستانه برای تلاشهای ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.
تعریف مشخصات کاربر	مدیر مجاز باید قادر به تعریف مشخصه های امنیتی بیشتر برای کاربران باشد.
مدیریت کلمه عبور	مدیریت تنظیمات و الزامات و قابلیتها برای تنظیم کلمه عبورها

مؤلفه	عملیات مدیریتی
احراز هویت کاربر	مدیریت داده های احراز هویت 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 شناسایی کاربران مدیریت تغییرات و فرایندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز میتواند قبل از شناسایی کاربر انجام دهد.
انقیاد مشخصه های امنیتی کاربر با موجودیت فعال متناظر	مدیر مجاز میتواند مشخصه های امنیتی موجودیتهای فعال پیش فرض را تعریف و تغییر دهد.
مدیریت مشخصه های امنیتی	مدیریت گروهی از نقشهایی که با مشخصه های امنیتی در تعامل هستند.
مقداردهی اولیه مشخصه ها	مدیریت گروهی از نقشهایی که مقادیر اولیه را مشخص میکنند .مدیریت مقادیر پیشفرض برای کنترل دسترسی محصول
مدیریت دادههای محصول -۱مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده های محصول
مدیریت داده های محصول -۱کاربر عادی، واردکننده داده	مدیریت گروهی از قوانینی مرتبط با داده های محصول
نقشهای 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 نشستها	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیشفرض غیرفعال بودن کاربر که نشست خاتمه یابد.

۳-۵-۵- کلاس حفاظت از توابع امنیتی هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FPT_FLS.۱	- -	۱	FPT_FLS.۱،۱	محصول باید در زمان رخداد انواع شکستهای زیر، وضعیت امن را حفظ نمایند : [**شکستهای نرم افزاری ، شکستهای سخت افزاری**]
	-	۲	FPT_ITT.۱،۱	محصول باید توانایی داشته باشد که در صورت فراهم نمودن بستر و زیرساخت امن، از افشاء یا تغییر داده در هنگام انتقال بین بخشهای مجزای خود که باهم ارتباط دارند، محافظت نماید.
FPT_TDC.۱	- -	۳	FPT_TDC.۱،۱	محصول در صورت استفاده از محصولات امن IT باید تفسیر سازگار [**کد تاییدیه برای احراز هویت دوعامله**]را در زمان اشتراک گذاری داده امنیتی بین خود و دیگر محصولات امن IT فراهم آورد
	-	٤	FPT_TDC.۱،۲	محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، [**APIبرای برقرار ارتباط با سروس پیامکی برای ارسال کد یکبار مصرف**] استفاده نماید.
	-	٥	FPT_STM.۱،۱	توابع امنیتی هدف ارزیابی باید قادر به ایجاد مهرهای زمانی قابل اطمینان باشند.
	-	٦	FPT_TUD_EXT.۱.۲	محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کارشناس شرکت تولیدکننده محصول فراهم کند که به روزرسانی نرم افزار و میان افزار محصول مورد ارزیابی را به صورت دستی آغاز کند و [از هیچ مکانیسم به‌روزرسانی پشتیبانی نکند]

٤-٥-٥- کلاس تخصیص منابع

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FRU_FLT.۱	- FPT_FLS.۱	۱	FRU_FLT.۱،۱	محصول باید از عملکرد[تمام کارکردهای اصلی]هنگام رویداد شکستهای زیر اطمینان حاصل کند: [**شکست نرم افزاری ، [هیچ نوع شکست دیگری]]**

۵-۵-۵- کلاس دسترسی به هدف ارزیابی

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTA_MCS.۱	FIA_UID.۱ -	۱	FTA_MCS.۱،۱	محصول باید حداکثر تعداد نشستهای همزمان متعلق به یک کاربر را محدود کند.
		۲	FTA_MCS.۱،۲	محصول باید به صورت پیش‌فرض، **[سه نشست همزمان پیش‌فرض]** برای هر کاربر در نظر بگیرد.
FTA_SSL.۳	- -	۳	FTA_SSL.۳،۱	محصول باید کلیه نشستهای تعاملی راه دور را پس از مدت زمان **[یک عدد صحیح به دقیقه که توسط مدیر تنظیم میشود]** غیرفعال بودن، خاتمه دهد.
FTA_SSL.٤	- -	٤	FTA_SSL.٤،۱	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه ی خاتمه نشست را بدهد.
FTA_TAH.۱	- -	٥	FTA_TAH.۱،۱	در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس [زمان، **[هیچ مشخصه]]** دیگر باشد
FTA_TAH.۱	- -	٦	FTA_TAH.۱،۲	در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید [تاریخ، زمان] آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد.
FTA_TAH.۱	- -	۷	FTA_TAH.۱،۳	توابع امنیتی هدف ارزیابی نباید اطلاعات تاریخچه دسترسی را از واسط کاربری پاک نماید، بدون اینکه به کاربر فرصتی داده شود تا اطلاعات را بازبینی نماید.
FTA_TSE.۱	- -	۸	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 ی دیگر**] ممانعت نماید

۶-۵-۵- کلاس کانال‌ها و مسیرهای مورد اعتماد

مؤلفه	وابستگی ها	شماره	المان	شرح المان
FTP-TRP.۱	-	۱	FTP_TRP.۱,۱	محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [**TLSو HTTPS**] مسیر ارتباطی امنی فراهم نماید تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه‌دور ایجاد شود که به طور منطقی از دیگر کلنال‌ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده‌های تبادلی حفاظت نماید و تغییرات را تشخیص دهد.
	-	۲	FTP_TRP.۱,۲	محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.
	-	۳	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.
	-	۴	FTP_ITC.۱,۱	محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل[**TLS**]میان خود و موجودیت IT معتبر، [سرور ممیزی، سرور احرازهویت، **[هیچ سرور دیگر]]** 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
	-	۵	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.
	-	۶	FTP_ITC.۱,۳	محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای[**خواندن و نوشتن هرنوع اطلاعات از پایگاه داده**]راه‌اندازی نماید.
	-	۷	FCS_TLSS_EXT.۱,۱	محصول باید [(RFC۵۲۴۶) TLS ۱,۲] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • [ ]

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ TLS_RSA_WITH_AES_۲۵٦_CBC_SHA مطابق با RFC ۳۲٦۸ ○ TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHAمطابق با RFC ۳۲٦۸ ○ TLS_DHE_RSA_WITH_AES_۲۵٦_CBC_SHAمطابق با RFC ۳۲٦۸ ○ TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHAمطابق با RFC ٤٤۹۲ ○ TLS_ECDHE_RSA_WITH_AES_۲۵٦_CBC_SHAمطابق با RFC ٤٤۹۲ ○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHAمطابق با RFC ۴۴۹۲ ○ TLS_ECDHE_ECDSA_WITH_AES_۲۵٦_CBC_SHAمطابق با RFC ۴۴۹۲ ○ TLS_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵٦مطابق با RFC ۵۲٤٦ ○ TLS_RSA_WITH_AES_۲۵٦_CBC_SHA۲۵٦مطابق با RFC ۵۲٤٦ ○ TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵٦مطابق با RFC ۵۲٤٦ ○ TLS_DHE_RSA_WITH_AES_۲۵٦_CBC_SHA۲۵٦مطابق با RFC ۵۲٤٦ ○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA۲۵٦مطابق با RFC ۵۲۸۹ ○ TLS_ECDHE_ECDSA_WITH_AES_۲۵٦_CBC_SHA۳۸٤مطابق با RFC ۵۲۸۹ ○ TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵٦مطابق با RFC ۵۲۸۹ ○ TLS_ECDHE_ECDSA_WITH_AES_۲۵٦_GCM_SHA۳۸٤ مطابق با RFC ۵۲۸۹

مؤلفه	وابستگی ها	شماره	المان	شرح المان
				○ TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹ ○ TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹ • هیچ مجموعه رمز دیگری]].
	-	۸	FCS_TLSS_EXT.۱،۲	محصول باید اتصال‌های کاربرانی را که درخواست SSL۱،۰، SSL۲،۰، SSL۳،۰، TLS۱،۰ و [هیچ کدام] دارند، رد نماید.
	-	۹	FCS_TLSS_EXT.۱،۳	محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [۳۰۷۲ بیت، ۴۰۹۶ بیت، یا هیچ اندازه دیگری] و [منحنی‌های NIST [secp۲۵۶r۱, secp۳۸۴r۱] و هیچ منحنی دیگری] ،[۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید.

۶-۵- الزامات تضمین امنیتی

الزامات عملکرد تضـــمین توصـــیف کننده چگونگی ارزیابی هدف ارزیابی اســـت. 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

٦- خلاصه مشخصات هدف ارزیابی

برای ورود به سیستم ابتدا کاربر باید نام کاربری و رمز عبور و اگر در سیستم احراز هویت چندگانه فعال باشید می‌تواند کد را خود را وارد نماید .(FIA_UAU.٥،٢و FIA_UAU.٥،١)

تنظیمی در سیستم وجود دارد که کاربر در صورت چند بار تلاش ناموفق برای ورود،غیر فعال میشود. بطور پیش فرض با وجود مقدار صفر، محدودیتی روی تعداد تلاش‌های ناموفق اعمال نمی‌گردد.(FIA_AFL.١،١, FIA_AFL.١،٢)

محصول مشخصه های امنیتی زیر را برای هر کاربر نگهداری مینماید:
شناسه کاربر،متد احرازهویت مورد استفاده،داده احرازهویت،نقش کاربر،وضعیت حساب کاربری(FIA_ATD.١،١, FIA_USB.١،١)
رمز عبور کاربر میتواند بعد از چند روز(قابل تنظیم) منقضی شده و کاربر باید آن را عوض کند.
سیاست گذر واژه را بر مبنای زیر می توان تعیین کرد:

١. رمز عبور نباید کمتر از ١٢ و بیشتر از ١٢٨ کاراکتر باشد.
٢. رمز عبور بصورت حساس (بزرگ و کوچک)کنترل شود.
٣. رمز عبور باید قوی باشد.
٤. رمز عبور باید خیلی قوی باشد.

برای تعیین سیاست گذرواژه ای تعیین کرد.(FIA_PMG_EXT.١،١)
محصول پیش از احراز هویت اجازه هیچ اقدامی به کاربر نمی‌دهد محصول هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احرازهویت می‌نماید.(FIA_UID.٢،١)
زمانی که کاربری login می‌کند در دستگاه دیگری با همان کد کاربری اجازه ورود ندارد.همچنین تنظیمی وجود دارد که حداکثر تعداد ورود همزمان یک کاربر را در یک دستگاه محدود میکند.البته برای هر ورود مجزا ،کاربر باید نام کاربری و کلمه عبور خود را وارد کند.(FTA_MCS.١,٢,FIA_USB.١،٢, FTA_MCS.١،١, FDP_ACF.١،٤)

محصول به کاربری که login کرده اجازه میدهد از آن خارج شود(FTA_SSL.٤،١)
تنظیمی در محصول وجود دارد که از تغییر مشخصه های امنیتی یک کاربر در حال کار جلوگیری می‌کندهمچنین تغییر نقش کاربر نیاز به ورود مجدد دارد(FIA_USB.١،٣)
همچنین مدت زمانی قابل تنظیم است که پس از سپری شدن آن،محصول کاربری که در آن مدت غیر فعال است را از Logout می‌کند و باید دوباره Login نماید.(FTA_SSL.٣،١)
تنظیمی در محصول وجود دارد که براساس نام کامپیوتر ،آدرس IP و تاریخی مشخص(از-تا) از ورود کاربران جلوگیری می‌کند(FTA_TSE.١،١)
تمامی فعالیت‌های مهم در سیستم لاگ می‌شود.

اطلاعاتی از قبیل ورود(موفق یا ناموفق) و خروج کاربر،تغییر در تنظیمات سیستم،تمامی برنامه های اجرا شده کاربران،تغییر در مدیریت کدها،ایجاد/تغییر کاربر یا گروه کاربری،تغییر دسترسی به کاربران و ... در سیستم لاگ می‌شود.(لیست تمامی مواردی که در سیستم لاگ می‌شوند در کد ۹۹۵۴ مدیریت کدها قراردارد) که در برنامه سوابق اطلاعات کاربر نمایش داده می‌شود.
در صورت رسیدن حجم لاگ به حد آستانه یا ماکزیمم حد خود رکورد لاگ ثبت می‌شود.در صورت زدن اشتباه کد احراز هویت چندعامله یا ثبت رمز عبوری که با سیاست رمز عبور تنظیم شده متناقض است هم رکورد لاگی ثبت می‌شود. در صورت دستکاری اطلاعات حساس در دیتابیس، توسط برنامه مانیتورینگ تغییرات اطلاعات حساس، تشخیص داده خواهد شد.
به ازای هر رکورد لاگ ،یک شناسه یکتا،تاریخ و زمان وقوع رویداد،نوع رویداد،کاربر ایجاد کننده، آی پی ،نام کاربر ،نام عملیات مربوطه و اطلاعات اضافه دیگری که برای هر نوع لاگ لازم است ذخیره می‌شود.(FAU_GEN.۱،۱, FAU_GEN.۱،۲, FAU_GEN.۲،۱)
در برنامه مانیتورینگ عملیات سیستم‌ها،امکان مشاهده لاگهای موجود در سیستم توسط سرپرست سیستم هست.در بالای فرم میتوانید لاگها را براساس تاریخ وقوع،نوع لاگ و سیستم مورد نظر فیلتر کنید.هم‌چنین می‌توانید براساس تمامی ستون‌های نمایش داده شده مرتب سازی کنید. همچنین در این برنامه عملیات ها مشاهده نشده و همچنین تاریخچه ای از تمام لاگها نمایش داده میشود.
در فرم مدیریت کدها،جداول عمومی ،جدول ۹۹۵۴ انواع لاگهای موجود در محصول تعریف شده اند که میتوان در اینجا یک نوع لاگ خاص را فعال/غیرفعال نمود یا امکان حذف این نوع لاگ را فراهم کرد. لازم به ذکر است در صورت غیر فعال بودن لاگ هیچ لاگ از کد مورد نظر در سیستم ثبت نمی‌شود.
(FAU_SAR.۱،۱, FAU_SAR.۱،۲, FAU_SAR.۲،۱, FAU_SAR.۳،۱, FAU_SEL.۱،۱)

امکان تغییر در ردیفهای لاگ در سیستم وجود ندارد.در لیست لاگهای آورده شده،در صورت وقوع هر تغییری در ردیف لاگ ذخیره شده، امکان مشاهده رکوردهای تغییر کرده، توسط برنامه مانیتورینگ تغییرات اطلاعات حساس وجود دارد. (FAU_STG.۱،۱, FAU_STG.۱،۲, FDP_SDI.۲،۱, FDP_SDI.۲،۲)

تنظیمی در سیستم وجود دارد که حد آستانه لاگ (حجم به مگابایت) تعریف شده و در صورت رسیدن جدول لاگ به این حجم، امکان ارسال پیغام به کاربر تعیین شده (SMS) وجود دارد.همچنین یک ردیف لاگ ثبت می‌شود.در صورت تغییر هر گونه اطلاعات مربوط به تنظیمات SMS باید سرویس Adaptor که با اسم Bll Hostشناخته می‌شود باید یک بار متوقف شود و دوباره اجرا شود. و همچین یک یوزر نیم تعریف شده است که در صورت تغییر مشخصات ورود این کاربر سرویس عملکرد درستی نخواد داشت.
همچنین تنظیم دیگری برای ماکزیمم حجم لاگ و همچنین تعداد رکوردهای لاگ برای حذف وجود دارد.در صورت رسیدن جدول لاگ به این حجم،به تعداد رکوردهای تنظیم شده از ابتدای جدول لاگ حذف شده و یک ردیف لاگ ثبت می‌شود.
برای فعالسازی این دو تنظیم باید از برنامه زمانبندی اجرای کدها که در مدیریت اطلاعات پایه،مدیریت سیستم‌ها قرار دارد استفاده نمود و همچنین دسترسی ها لازم به یوزر تعریف شده برای حذف لاگ داده شود تا سرویس به دسترسی عمل کند و همچنین کافی است در این برنامه دکمه نصب را بزنیم تا دو تنظیم فوق بصورت سرویس دردستگاه فایل سرور نصب گردند.در هنگام نصب سرویس مدت زمان زمانبندی اجرای کدها قابل تنظیم است.

(FAU_STG.۳،۱, FAU_STG.٤،۱)

در سیستم نقشهای کاربر عادی و سرپرست سیستم وجوددارد(FMT_SMR.۱،۱)

در برنامه مدیریت کاربران میتوان عملیات زیر را انجام داد:

- امکان ایجاد/مشاهده/تغییر گروه کاربران
- مشاهده کاربران سیستم و تغییر مشخصه های آنها(نام کاربری و کلمه عبور،فعال بودن ، سرپرست بودن)
- امکان دادن/برداشتن دسترسی برنامه های سیستم به کاربر یا گروه کاربر

میتوان یک گروه کاربری تعریف کرد(مانند کاربران واحد حسابداران)،کاربران مربوطه را به این گروه تخصیص داد و دسترسی برنامه ها(فرمها)ی مورد نیاز را به این گروه داد(لازم نیست به تک تک کاربران دسترسی داده شود).

در سیستم با استفاده از SHA-۲٥٦ برای وارسی صحت داده ها ممیزی را رمزنگاری می‌کند(, FCS_COP.۱،۱(۱) ((۲)FCS_COP.۱،۱

مجصول با واسط کاربری که به آن اختصاص داده شده است میتوان خط مشی های کنترل دسترسی را بر روی موارد زیر اعمال می‌کند و هنگام استفاده از محصول از این خط مشی ها استفاده شده است تا کنترل دسترسی کاربران را کنترل نماید: موجودیت فعال (مدیر سیستم و کاربر عادی) و موجودیت غیرفعال (رکوردها، مستندات و فرا-داده و داده متعلق به کاربران و داده احرازهویت و داده با این معیارها) و عملیات (ایجاد موجودیت غیرفعال جدید و حذف موجودیت غیرفعال و تغییر دسترسیها به موجودیت غیرفعال و عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال) و هویت کاربر و نقش ها و مجوز های کاربر مجاز و اطلاعات نشست کاربر و پارامتر هایی که با درخواست فرستاده می‌شوند (FDP_ACC.۱،۱, FDP_ACF.۱،۱)

محصول قوانین زیر را بر روی موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده با استفاده از تنظمیاتی که در بخش مجوز ها و کاربران میتواند قوانین زیر اعمال کند :

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 و همچنین کاربران با مجوز مدیر سیستم به رکوردهای لازمه مدیریت سیستم و نیز روش ارائه شده توسط محصول، دسترسی دارند و کاربران غیرمجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند.(FDP_ACF.۱،۱, FDP_ACF.۱،۳)

محصول 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_RIP.۲،۱)

محصول پیش از احراز هویت کاربر اجازه هیچ عملیاتی به کاربر را نمیدهد.(FIA_UAU.۲،۱)

محصول به گونه‌ای طراحی و پیاده‌سازی شده است که مدیر سیستم و هر کاربری که مجوز لازم را دارد می‌تواند رفتار توابع مدیریت محصول را تعیین، فعال، غیرفعال و تغییر دهد. این فرآیند با اعمال خط‌مشی‌های کنترل دسترسی و بررسی دقیق دسترسی‌ها و خط‌مشی‌های تنظیم شده برای هر درخواست انجام می‌شود. اقدامات زیر در محصول به منظور حفظ امنیت و مدیریت کارکردها انجام شده است:

۱. محدودیت دسترسی به مدیریت رفتار توابع:(FMT_MOF.۱،۱) تنها مدیر سیستم و کاربران دارای مجوز قادر به تعیین، فعال یا غیرفعال کردن و تغییر رفتار توابع مدیریت محصول هستند.هر درخواست از هر کاربر بررسی می‌شود و در صورت عدم تطابق با خط‌مشی‌ها و دسترسی‌ها، عملیات متوقف می‌شود.

۲. اعمال خط‌مشی‌های کنترل دسترسی:(FMT_MSA.۱،۱) خط‌مشی‌های کنترل دسترسی برای تغییر پیش‌فرض، پرس و جو، تغییر، و حذف مشخصه‌های امنیتی نقش‌ها و مجموعه دسترسی‌های کاربران اعمال می‌شود.تنها مدیر سیستم و کاربران دارای مجوز قادر به تغییر این خط‌مشی‌ها هستند.

۳. مدیریت داده‌های سیستم:((FMT_MTD.۱،۱(۱), FMT_MTD.۱،۱(۲)) سیستم قابلیت پرس‌وجو، تغییر، و حذف داده‌های ممیزی و حفاظت از داده‌های کاربری را دارد.تنها مدیر سیستم و کاربران دارای مجوز قادر به انجام این عملیات هستند.

٤. قابلیت انجام تمام کارکردهای مدیریتی:(FMT_SMF.۱،۱) محصول قادر به انجام تمامی کارکردهای مدیریتی که در جدول دو آمده است، می‌باشد.مدیر سیستم و کاربران دارای مجوز می‌توانند کاربران با نقش‌ها و دسترسی‌های مجاز را تعریف و مدیریت کنند.

۵. مدیریت نقش‌ها و دسترسی‌ها:(FMT_SMR.۱،۲) محصول امکان تعریف و مدیریت نقش‌ها و دسترسی‌های کاربران را دارد.دسترسی به این کارکردها تنها برای مدیر سیستم و کاربران دارای مجوز ممکن است.

این اقدامات تضمین می‌کنند که تنها افراد مجاز قادر به مدیریت و تغییر رفتار توابع محصول و داده‌های حساس هستند و هرگونه تلاش برای دسترسی غیرمجاز به داده‌ها و توابع مدیریتی با شکست مواجه می‌شود.

محصول به گونه‌ای طراحی و پیاده‌سازی شده است که تنظیمات دسترسی و مشخصه‌های امنیتی با مقادیر پیش‌فرض محدود شده‌ای ارائه می‌شوند. این مقادیر پیش‌فرض به گونه‌ای انتخاب شده‌اند که امنیت سیستم را در حد مطلوبی نگه دارند و تنها در صورت نیاز توسط مدیر سیستم تغییر داده می‌شوند. اقدامات زیر در محصول برای مدیریت این تنظیمات انجام شده است:

مقادیر پیش‌فرض محدود شده برای مشخصه‌های امنیتی (FMT_MSA.۳،۱):محصول مقادیر پیش‌فرض محدود شده‌ای را برای مشخصه‌های امنیتی در نظر می‌گیرد تا از اعمال خط‌مشی‌های امنیتی مناسب اطمینان حاصل شود.

این مقادیر پیش‌فرض به گونه‌ای تنظیم شده‌اند که دسترسی‌ها و مجوزها به صورت محدود و کنترل شده تعریف شوند.

امکان تغییر مقادیر پیش‌فرض توسط مدیر سیستم (FMT_MSA.۳،۲):مدیر سیستم می‌تواند در صورت نیاز، مقادیر پیش‌فرض را تغییر دهد و خط‌مشی‌های مناسب‌تری را اعمال کند.

تعیین مقادیر اولیه پیشنهادی به مدیر سیستم این امکان را می‌دهد که هنگام ایجاد اطلاعات یا موجودیت‌های جدید، مقادیر پیش‌فرض را لغو و تغییر دهد تا با نیازهای خاص سازمان سازگار شود.

این تنظیمات تضمین می‌کنند که محصول به صورت پیش‌فرض با مقادیر امنیتی مناسبی کار می‌کند و در عین حال، انعطاف‌پذیری لازم را برای تغییر این مقادیر توسط مدیر سیستم فراهم می‌کند تا متناسب با نیازهای امنیتی خاص تنظیم شود..

محصول مورد نظر به گونه‌ای طراحی و پیاده‌سازی شده است که در صورت بروز شکست‌های نرم‌افزاری و سخت‌افزاری، با استفاده از مکانیزم‌های مدیریت خطا(Error Handling) ، وضعیت امن خود را حفظ می‌نماید. برای دستیابی به این هدف، اقدامات زیر انجام شده است (FPT_FLS.۱،۱, FPT_TUD_EXT.۱،۲)

۱. مدیریت خطاهای نرم‌افزاری :در هنگام بروز خطاهای نرم‌افزاری، محصول از طریق مکانیزم‌های پیش‌بینی شده به گونه‌ای عمل می‌کند که از افشاء اطلاعات حساس یا دسترسی غیرمجاز به سیستم جلوگیری شود. این شامل:

- تشخیص و گزارش خطا :سیستم به صورت خودکار خطاها را تشخیص داده و گزارش می‌کند.
- واکنش مناسب به خطا :در صورت بروز خطا، سیستم به حالت امن بازمی‌گردد و عملیات مشکوک متوقف می‌شود.

۲. مدیریت خطاهای سخت‌افزاری :در هنگام بروز شکست‌های سخت‌افزاری، محصول از طریق مکانیزم‌های متعددی وضعیت امن خود را حفظ می‌نماید. این شامل:

- تشخیص خودکار شکست‌های سخت‌افزاری :سیستم به صورت مداوم عملکرد سخت‌افزار را نظارت می‌کند و شکست‌ها را تشخیص می‌دهد.
- پاسخ مناسب به شکست‌های سخت‌افزاری :در صورت شناسایی شکست سخت‌افزاری، سیستم به حالت امن بازمی‌گردد و از دسترسی غیرمجاز جلوگیری می‌شود.

۳. به‌روزرسانی امن سیستم :(FPT_TUD_EXT.۱،۲) محصول امکان به‌روزرسانی امن را فراهم کرده است تا در صورت بروز خطاهای نرم‌افزاری، با به‌روزرسانی‌های مناسب مشکلات برطرف شوند. این شامل:

- به‌روزرسانی امن نرم‌افزار :تمامی به‌روزرسانی‌ها از طریق کانال‌های امن منتقل و اعمال می‌شوند.
- اعتبارسنجی به‌روزرسانی‌ها :به‌روزرسانی‌ها پیش از اعمال، اعتبارسنجی شده تا از صحت و امنیت آنها اطمینان حاصل شود.

محصول مورد نظر به گونه‌ای طراحی و پیاده‌سازی شده است که از افشاء یا تغییر داده در هنگام انتقال بین بخش‌های مجزای خود که با یکدیگر در ارتباط هستند، جلوگیری کند. برای دستیابی به این هدف، اقدامات زیر انجام شده است(FPT_ITT.۱،۱):

۱. استفاده از پروتکل‌های امن انتقال داده :پروتکل‌های امن مانند TLS/SSL برای رمزگذاری داده‌ها در هنگام انتقال به کار گرفته شده‌اند تا از شنود یا تغییر داده‌ها توسط افراد غیرمجاز جلوگیری شود.

۲. تصدیق هویت مبدأ و مقصد :به منظور اطمینان از این‌که داده‌ها فقط بین بخش‌های مجاز منتقل می‌شوند، از مکانیزم‌های تصدیق هویت (Authentication) قوی استفاده شده است.

۳. استفاده از الگوریتم‌های رمزنگاری قوی :الگوریتم‌های رمزنگاری استلندارد و قوی مانند AES برای رمزگذاری داده‌های حساس به کار رفته است.

٤. کنترل دسترسی به داده‌ها :دسترسی به داده‌های در حال انتقال تنها به افراد و سیستم‌های مجاز داده شده و از مکانیزم‌های کنترل دسترسی مناسب استفاده شده است.

۵. نظارت و گزارش‌گیری از انتقال داده‌ها :تمامی عملیات انتقال داده‌ها به صورت مداوم نظارت شده و گزارش‌های مربوط به تلاش‌های ناموفق برای دسترسی به داده‌ها ذخیره و تحلیل می‌شوند.

محصول با استفاده از محصولات امن IT باید تفسیر سازگار کد تاییدیه برای احراز هویت دوعامله را در زمان اشتراک‌گذاری داده‌های امنیتی بین خود و دیگر محصولات امن IT فراهم آورد. برای دستیابی به این هدف، اقدامات زیر انجام شده است(FPT_TDC.۱،۱):

۱. استفاده از احراز هویت دوعامله :(۲FA) محصول از مکانیزم‌های احراز هویت دوعامله برای اطمینان از صحت و امنیت هویت کاربران استفاده می‌کند. این مکانیزم شامل استفاده از کدهای تاییدیه ارسال شده به دستگاه‌های مطمئن یا از طریق اپلیکیشن‌های احراز هویت است.

۲. تفسیر سازگار کد تاییدیه :محصول قادر است کدهای تاییدیه ارسال شده از محصولات امن IT دیگر را به طور سازگار تفسیر و پردازش کند. این اطمینان را می‌دهد که کدهای تاییدیه به درستی توسط هر دو طرف فرستنده و گیرنده شناسایی و تایید می‌شوند.

۳. اشتراک‌گذاری امن داده‌های امنیتی :در هنگام اشتراک‌گذاری داده‌های امنیتی بین محصولات امنIT ، محصول از پروتکل‌های امن برای انتقال داده‌ها استفاده می‌کند. این شامل رمزگذاری داده‌ها و استفاده از کانال‌های امن برای جلوگیری از افشاء یا تغییر داده‌ها است.

٤. تصدیق هویت و کنترل دسترسی :محصول از مکانیزم‌های تصدیق هویت قوی برای اطمینان از این‌که تنها کاربران و سیستم‌های مجاز قادر به دسترسی و اشتراک‌گذاری داده‌های امنیتی هستند، استفاده می‌کند.

محصول باید قابلیت ایجاد مهرهای زمانی دقیق و قابل اطمینان را داشته باشد تا بتواند فعالیت‌ها و رخدادهای سیستم را به‌طور صحیح ثبت و ردیابی کند(FPT_STM.۱,۱):

استفاده از سرورهای زمان معتبر: برای اطمینان از دقت و صحت زمان، سرورهای ویندوز به‌عنوان منبع زمان سیستم انتخاب و پیکربندی شدند استفاده میشود.

ثبت دقیق رخدادها: تمامی رخدادهای مهم سیستم با استفاده از مهرهای زمانی دقیق ثبت می‌شوند تا امکان ردیابی و تحلیل دقیق فعالیت‌ها فراهم باشد.

کنترل دسترسی به زمان سیستم: دسترسی به تنظیمات زمان سیستم محدود به کاربران مجاز و نقش‌های مدیریتی شده است تا از دستکاری‌های غیرمجاز جلوگیری شود.

پشتیبان‌گیری منظم: نسخه‌های پشتیبان از تنظیمات زمان و اطلاعات رخدادها به‌طور منظم تهیه و ذخیره می‌شوند تا در صورت نیاز امکان بازیابی اطلاعات فراهم باشد.

این زیر اطمینان می‌دهند که محصول به الزامات امنیتی FTA_TAH.۱,۲ ,FTA_TAH.۱,۱ و FTA_TAH.۱,۳ به‌طور کامل پاسخ می‌دهد و امنیت نشست‌ها و تاریخچه دسترسی کاربران را تضمین می‌کند.

۱. نمایش آخرین تلاش موفق:پس از برقراری موفقیت‌آمیز هر نشست کاربری، تاریخ و زمان آخرین تلاش موفق برای ایجاد نشست به کاربر نمایش داده می‌شود.

۱ اطلاع‌رسانی درباره تلاش‌های ناموفق:در هنگام برقراری نشست موفق، توابع امنیتی تاریخ و زمان آخرین تلاش ناموفق برای برقراری نشست را نمایش می‌دهند.تعداد تلاش‌های ناموفق از زمان آخرین نشست موفق نیز به کاربر اطلاع داده می‌شود.

۲ حفظ اطلاعات تاریخچه دسترسی:اطلاعات تاریخچه دسترسی کاربران بدون حذف از واسط کاربری نگهداری می‌شوند، به‌طوری که کاربر فرصت بازبینی و بررسی این اطلاعات را دارد.

۳ روندهای امنیتی در مدیریت نشست‌ها:تمامی اطلاعات مربوط به تلاش‌های موفق و ناموفق برای ایجاد نشست، به‌صورت امن و قابل دسترس در لاگ‌های سیستم ذخیره می‌شود.کاربر نمی‌تواند بدون مشاهده و بازبینی این اطلاعات، آنها را از واسط کاربری پاک کند، تا از دسترسی و آگاهی کامل از تاریخچه فعالیت‌های خود مطمئن باشد.

٤ رعایت حریم خصوصی و امنیت اطلاعات:تمامی اطلاعات ذخیره شده از تلاش‌های موفق و ناموفق به‌طور امن و با رعایت اصول حریم خصوصی کاربران مدیریت و نگهداری می‌شود.

تمامی ارتباطات میان محصول و موجودیت‌های معتبر IT، از جمله سرور ممیزی و سرور احرازهویت، با استفاده از پروتکل TLS و TDS برقرار می‌شود.

احرازهویت موجودیت‌ها:محصول فرآیند احرازهویت را برای تمامی موجودیت‌های IT معتبر پیاده‌سازی می‌کند تا مطمئن شود که تنها موجودیت‌های مجاز قادر به برقراری ارتباط با سیستم هستند.

تشخیص تغییرات:مکانیزم‌های تشخیص تغییرات برای بررسی صحت و تمامیت داده‌های تبادلی به‌کار گرفته شده‌اند. این مکانیزم‌ها هرگونه تغییر غیرمجاز در داده‌ها را شناسایی می‌کنند.

اجازه برقراری ارتباط از طریق کانال امن:محصول به موجودیت‌های معتبر IT اجازه می‌دهد که ارتباطات را از طریق کانال امن آغاز کنند، این امکان از طریق تنظیمات امنیتی و پیکربندی‌های مخصوص فراهم شده است.

خواندن و نوشتن اطلاعات پایگاه داده:تمامی عملیات خواندن و نوشتن اطلاعات از پایگاه داده، از طریق کانال امن انجام می‌شود تا امنیت داده‌ها در هنگام انتقال تضمین شود.

تمایز منطقی کانال‌ها:کانال‌های ارتباطی امن از نظر منطقی از سایر کانال‌ها متمایز شده‌اند تا تداخل و نفوذ احتمالی به حداقل برسد.این اقدامات اطمینان می‌دهند که محصول به الزامات امنیتی FTP_ITC.۱،۲ ,FTP_ITC.۱،۱ و FTP_ITC.۱،۳ به‌طور کامل پاسخ می‌دهد و ارتباطات امن و مطمئنی را میان محصول و موجودیت‌های معتبر IT فراهم می‌کند.

این اقدامات زیر اطمینان می‌دهند که محصول به الزامات امنیتی FDP_ACF.۱،۲ به‌طور کامل پاسخ می‌دهد و عملیات بین موجودیت‌های فعال و غیرفعال به‌صورت امن و مطابق با قوانین کنترل دسترسی مجاز شناخته می‌شوند.

۱. ایجاد و نگهداری لیست کنترل دسترسی:لیست کنترل دسترسی (ACL) شامل رکوردهایی است که حقوق دسترسی کاربران، گروه‌ها و نقش‌ها را به موجودیت‌های غیرفعال تعریف می‌کند.

۲. احراز هویت و مجوزدهی:هر کاربر یا موجودیت فعال، پیش از انجام هر عملیات، احراز هویت شده و شناسه کاربری، گروه یا نقش او بررسی می‌شود.

۳. بررسی لیست کنترل دسترسی:هنگام درخواست عملیات توسط موجودیت فعال، محصول لیست کنترل دسترسی را بررسی می‌کند تا اطمینان حاصل کند که رکورد مربوط به حق دسترسی موجود است.اگر رکوردی موجود باشد که حق دسترسی لازم را برای کاربر یا گروه یا نقش کاربری تعریف کرده باشد، عملیات مجاز شناخته می‌شود و انجام می‌گیرد.در صورت عدم وجود رکورد مناسب در لیست کنترل دسترسی، عملیات رد می‌شود و به کاربر اطلاع‌رسانی می‌شود که دسترسی مجاز نیست.

٤. ثبت و پایش:تمامی تلاش‌های دسترسی، چه موفق و چه ناموفق، در لاگ‌های سیستم ثبت می‌شوند تا امکان پایش و بررسی دقیق‌تر فراهم باشد.

٥. مدیریت پویا:لیست کنترل دسترسی به‌صورت پویا و مداوم مدیریت و به‌روزرسانی می‌شود تا تغییرات در حقوق دسترسی کاربران، گروه‌ها و نقش‌ها به‌سرعت اعمال شوند.

٦. اعمال اصول کمترین امتیاز:به منظور افزایش امنیت، اصول کمترین حق دسترسی (Least Privilege) در طراحی لیست کنترل دسترسی رعایت می‌شود، به‌طوری که کاربران تنها به منابع و عملیات مورد نیاز دسترسی داشته باشند.

محصول باید هنگام ورود و خروج داده‌های کاربری، خط‌مشی‌های کنترل دسترسی و مشخصه‌های امنیتی مرتبط را اعمال و مدیریت کند.(FDP_ITC.۲،۱ و FDP_ITC.۲،۱ و FDP_ITC.۲،۳ و FDP_ITC.۲،٤ و FDP_ETC.۲،۱ و FDP_ETC.۲،۲ و FDP_ETC.۲،۳ و FDP_ETC.۲،٤)

اعمال خط‌مشی کنترل دسترسی:هنگام دریافت یا خروج داده‌های کاربری، محصول خط‌مشی کنترل دسترسی را اعمال می‌کند تا اطمینان حاصل شود که تنها کاربران مجاز قادر به دسترسی و انتقال داده‌ها هستند.

مدیریت مشخصه‌های امنیتی هنگام وارد کردن داده:محصول مشخصه‌های امنیتی مانند نوع داده، حجم و اندازه فایل، فرمت فایل و تعداد دفعات وارد کردن (Import) را ذخیره و بررسی می‌کند.

پروتکل‌های استفاده‌شده برای انتقال داده‌ها، ارتباط و همبستگی شفافی بین مشخصه‌های امنیتی و داده‌های کاربری دریافت شده ایجاد می‌کنند.اطمینان حاصل می‌شود که تفسیر مشخصه‌های امنیتی داده‌های کاربری مطابق با مقصود فرستنده است.

مدیریت مشخصه‌های امنیتی هنگام خروج داده:مشخصه‌های امنیتی مرتبط با داده‌های کاربری به همراه داده‌های خروجی منتقل می‌شوند.

اطمینان حاصل می‌شود که مشخصه‌های امنیتی هنگام خروج داده، ارتباط و پیوند شفافی با داده‌های خارج شده دارند.

مدیر سیستم باید خروج رکوردها را محدود کند تا کاربران نتوانند بدون هدف مشخص داده‌ها را از محصول خارج کنند.

محصول می‌تواند از API برای تفسیر داده‌های دریافتی از دیگر محصولات IT امن استفاده کند، به‌طوری که بتواند ارتباطی با سرویس پیامکی برقرار کند و کد یکبار مصرف را برای ارسال به کاربران استفاده کند.(FPT_TDC.۱،۲)

بررسی و تفسیر داده‌های دریافتی:محصول به‌صورت امن و با استفاده از API، داده‌های دریافتی از دیگر محصولات IT را بررسی و تفسیر می‌کند.

ارسال کد یکبار مصرف از طریق سرویس پیامکی:با استفاده از API، محصول قادر است ارتباطی با سرویس پیامکی برقرار کند و کدهای یکبار مصرف را برای ارسال به کاربران استفاده نماید.

محصول باید از عملکرد تمامی کارکردهای اصلی خود در صورت رخداد شکست نرم‌افزاری اطمینان حاصل کند، به‌طوری که امکان ادامه وظایف و عملکرد نرم‌افزار در شرایط ناپیش‌بینی فراهم شود.(FRU_FLT.۱،۱):
مانیتورینگ و پایش: سیستم محصول برای شناسایی و پایش شکست‌های نرم‌افزاری به‌کار می‌رود.
نگهداری لاگ‌ها و ثبت خطاها برای تجزیه و تحلیل بعدی از شکست‌های نرم‌افزاری.
بهبود پایداری سیستم: اعمال بهینه‌سازی‌ها و به‌روزرسانی‌های لازم به منظور کاهش احتمال وقوع شکست‌های نرم‌افزاری.
آزمون‌های توسعه داده‌شده و یکپارچه برای اطمینان از عملکرد صحیح و پایدار سیستم.
استراتژی مدیریت خطا:تعیین استراتژی‌ها و فرآیندهای مناسب برای مدیریت و رفع خطاها در سریع‌ترین زمان ممکن.
ارتقاء قابلیت‌های بازیابی و پشتیبانی به منظور حفظ ادامه فعالیت‌ها و کاهش تأثیر شکست‌های نرم‌افزاری بر کاربران.

محصول می‌تواند پروتکل HTTPS را مطابق با RFC ۲۸۱۸ و با استفاده از TLS اجرا کند. در صورتی‌که گواهی‌نامه همتا ارائه شده نامعتبر باشد، محصول اتصال را برقرار نمی‌کند، برای برقراری اتصال درخواست مجوز می‌نماید و هیچ اقدام دیگری انجام نمی‌دهد. (FCS_HTTPS_EXT.۱،۱، FCS_HTTPS_EXT.۱،۲، FCS_HTTPS_EXT.۱،۳)

محصول می‌تواند TLS ۱،۲ (مطابق با RFC ۵۲٤٦) را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند.
همچنین، TLS با پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی می‌شود:
TLS_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۳۲٦۸
TLS_RSA_WITH_AES_۱۹۲_CBC_SHA مطابق با RFC ۳۲٦۸
TLS_RSA_WITH_AES_۲۵٦_CBC_SHA مطابق با RFC ۳۲٦۸
TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ۳۲٦۸
TLS_DHE_RSA_WITH_AES_۱۹۲_CBC_SHA مطابق با RFC ۳۲٦۸
TLS_DHE_RSA_WITH_AES_۲۵٦_CBC_SHA مطابق با RFC ۳۲٦۸
TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ٤٤۹۲
TLS_ECDHE_RSA_WITH_AES_۱۹۲_CBC_SHA مطابق با RFC ٤٤۹۲
TLS_ECDHE_RSA_WITH_AES_۲۵٦_CBC_SHA مطابق با RFC ٤٤۹۲
TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA مطابق با RFC ٤٤۹۲
TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_CBC_SHA مطابق با RFC ٤٤۹۲
TLS_ECDHE_ECDSA_WITH_AES_۲۵٦_CBC_SHA مطابق با RFC ٤٤۹۲
TLS_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵٦ مطابق با RFC ۵۲٤٦
TLS_RSA_WITH_AES_۱۹۲_CBC_SHA۲۵٦ مطابق با RFC ۵۲٤٦
TLS_RSA_WITH_AES_۲۵٦_CBC_SHA۲۵٦ مطابق با RFC ۵۲٤٦
TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵٦ مطابق با RFC ۵۲٤٦

TLS_DHE_RSA_WITH_AES_۱۹۲_CBC_SHA۲۵۶ مطابق با RFC ۵۲۴۶
TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA۲۵۶ مطابق با RFC ۵۲۴۶
TLS_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۸
TLS_RSA_WITH_AES_۱۹۲_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۸
TLS_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۸
TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶ مطابق با RFC ۵۲۸۹
TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_CBC_SHA۲۵۶ مطابق با RFC ۵۲۸۹
TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA۳۸۴ مطابق با RFC ۵۲۸۹
TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹
TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹
TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹
TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹
TLS_ECDHE_RSA_WITH_AES_۱۹۲_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹
TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹
TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶ مطابق با RFC ۵۲۸۹
TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶ مطابق با RFC ۵۲۸۹
TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA۳۸۴ مطابق با RFC ۵۲۸۹

محصول می‌تواند تنها در صورتی که گواهینامه سرور معتبر باشد، کانال امن را برقرار سازد و در صورت نامعتبر بودن گواهینامه سرور، ارتباط را برقرار نمی‌سازد. همچنین، مطابقت شناسه ارائه شده با شناسه مرجع مطابق بخش ۶ از RFC ۶۱۲۵ تأیید می‌شود. (FCS_TLSC_EXT.۱،۱، FCS_TLSC_EXT.۱،۲، FCS_TLSC_EXT.۱،۳)

محصول می‌تواند Extension Elliptic Curves را به همراه NISTهای secp۲۵۶r۱، secp۳۸۴r۱، secp۵۲۱r۱ در پیام ClientHello ارائه دهد و هیچ منحنی دیگری پشتیبانی نمی‌شود. (FCS_TLSC_EXT.۴،۱)
محصول می‌تواند اتصال‌های کاربرانی را که درخواست SSL۱،۰، SSL۲،۰، SSL۳،۰، TLS۱،۰ و TLS۱،۱ دارند، رد نماید. (FCS_TLSS_EXT.۱،۲)

محصول می‌تواند پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت یا هیچ اندازه دیگری و منحنی‌های NIST secp۲۵۶r۱، secp۳۸۴r۱ ایجاد نماید. (FCS_TLSS_EXT.۱،۳)

محصول می‌تواند گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند:

- تأیید گواهی‌نامه مطابق با RFC ۵۲۸۰ و تأیید مسیر گواهی‌نامه با حداقل طول مسیر دو گواهی‌نامه.
- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.

- برای تأیید یک مسیر گواهی‌نامه، افزونه basic Constraints باید وجود داشته و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت "True"تنظیم‌شده باشد.
- وضعیت فسخ گواهی‌نامه با استفاده از پروتکل) OCSP مطابق با (RFC ٦٩٦٠ تأیید می‌شود.
- فیلد extendedKeyUsage بر اساس قوانین زیر تأیید می‌شود:
  - گواهی‌نامه‌های مورد استفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف "Code Signing"را در فیلد extendedKeyUsage داشته باشند.
  - گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" را در فیلد extendedKeyUsage داشته باشند.
  - گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" را در فیلد extendedKeyUsage داشته باشند.
  - گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف "OCSP Signing" را در فیلد extendedKeyUsageداشته باشند.

محصول تنها درصورتی‌که افزونه basic Constraints از پیش تنظیم‌شده باشد و پرچم CA به حالت "TRUE" تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد(FIA_X۵۰۹_EXT.۱،۱/Rev, FIA_X۵۰۹_EXT.۱،۲/Rev) .

محصول برای پشتیبانی از احراز هویت برای TLS و HTTPS، از گواهی‌نامه‌های X.۵۰۹v۳ تعریف‌شده در RFC ۵۲۸۰ استفاده می‌کند. در صورتی هدف امنیتی ارزیابی قادر به برقراری ارتباط جهت تعیین اعتبار گواهی دیجیتال نباشد، توابع امنیتی هدف ارزیابی باید به مدیر سیستم این امکان را بدهد که در زمینه‌ی پذیرش گواهی تصمیم‌گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد.(FIA_X۵۰۹_EXT.۲،۱ , FIA_X۵۰۹_EXT.۲،۲)

محصول می‌تواند در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل‌های TLS و HTTPS، مسیر ارتباطی امنی فراهم نماید. این امکان باعث می‌شود تا یک کانال ارتباطی بین محصول و کاربران راه‌دور ایجاد شود که به‌طور منطقی از دیگر کانال‌ها متمایز بوده، کاربر مربوطه را احراز هویت کرده و از تغییر و افشاء داده‌های تبادلی حفاظت نماید و تغییرات را تشخیص دهد. (FTP_TRP.۱،۱)

محصول می‌تواند به مدیر سیستم معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کند. این امر تضمین می‌کند که تنها مدیران سیستم معتبر قادر به آغاز ارتباطات حساس هستند. (FTP_TRP.۱،۲)

محصول می‌تواند استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه‌دور مدیر سیستم الزامی نماید. این الزام به منظور افزایش امنیت و جلوگیری از دسترسی‌های غیرمجاز به سیستم است. (FTP_TRP.۱،۳)

بخش توجیهات

الزامات زیر مربوط به پروفایل حفاظتی برنامه کاربردی تحت شبکه در محصول پیاده سازی نمیشوند:

شماره الزام	شرح	المان	توضیحات
۵۱f	به‌روز رسانی امن ۳	FPT_TUD_EXT.۱. ۳	در این محصول امکان به روز رسانی خودکار وجود ندارد.