به نام خدا

پروفایل حفاظتی سوئیچ KVM

نسخه ۲

مرداد ۱۳۹۳

پیش‌گفتار

این سند توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است که معرفی کننده الزامات کارکرد امنیتی برای سوئیچ‌های KVM می‌باشد تا تولیدکنندگان این سوئیچ‌ها بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ نموده و نیز سند هدف امنیتی[1] آن را ارائه نمایند.

در بخش معرفی محصول، سوئیچ KVM به صورت کلی معرفی شده است. سپس در قسمتی تحت عنوان «مسائل امنیتی» تهدیدهایی که محصول با آن‌ها روبرو است و فرضیاتی که در رابطه با امنیت محصول در نظر گرفته شده است و همچنین خط‌مشی‌های آن عنوان می‌شود. در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدها، اجرای خط مشی‌ها و بکاربردن فرضیات مطرح می‌شود. در ادامه «الزامات کارکرد امنیتی» آورده شده است. براساس استاندارد معیار مشترک این قسمت از چندین کلاس تشکیل شده است که هریک از این کلاس‌ها حوزه خاصی از امنیت را پوشش می‌دهد. کلاس‌هایی که برای سوئیچ KVM در این بخش از سند مطرح شده است عبارتند از:

- کلاس حفاظت از داده‌های کاربری
- کلاس مدیریت امنیت
- الزامات توسعه یافته
- هر کلاس مجموعه‌ای از خانواده و هر خانواده مجموعه‌ای از مؤلفه و هر مؤلفه مجموعه‌ای از عناصر می‌باشد. با استفاده از «الزامات کارکرد امنیتی» در واقع «اهداف امنیتی» بر مبنای استاندارد معیار مشترک بیان می‌شود.

1 Security Target (ST)

- در بخش پایانی «الزامات تضمین امنیتی» که از ساختاری مشابه بخش قبلی برخوردار است مطرح گردیده است، این بخش الزامات لازم جهت ارزیابی محصول را عنوان می‌کند.

فهرست

۱. هدف از ارائه سند

در راستای ارزیابی امنیتی محصولات مبتنی بر «استاندارد ارزیابی معیار مشترک» لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده نمودن الزامات ارائه شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود.

۲. معرفی اصطلاحات

- **هدف ارزیابی (TOE)**

به سیستم مورد ارزیابی براساس «استاندارد ارزیابی معیار مشترک»، هدف ارزیابی گفته می‌شود.

- **غیر هدف ارزیابی (Non-TOE[1])**

سخت‌افزار، نرم‌افزار و میان افزاری که هدف ارزیابی جهت اجرا به آن‌ها نیز نیاز دارد.

- **محیط عملیاتی (Operational Environment)**

محیطی که هدف ارزیابی در آن عمل می‌کند.

- **پروفایل حفاظتی (PP[2])**

بیانیه‌ای از الزامات امنیتی برای یک نوع از هدف ارزیابی، که الزامات امنیتی را به صورت کلی بیان می‌دارد.

1 Non-Target Of Evaluation
2 Protection Profile

- **هدف امنیتی (ST[1])**

بیانیه‌ای از الزامات امنیتی برای هدف ارزیابی خاصی، که الزامات امنیتی را به صورت جزئی‌تر بیان می‌دارد. این بیانیه معمولاً توسط سازنده هدف ارزیابی نوشته می‌شود.

- **مسائل امنیتی (Security Problem)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «مشکل امنیتی» وجود دارد که به طور رسمی ماهیت و حوزه امنیت در نظر گرفته شده توسط هدف ارزیابی را تعریف می‌کند.

این بیانیه شامل موارد زیر است:

- «تهدیدهایی» که توسط هدف ارزیابی و محیط عملیاتی‌اش مقابله می‌شود.
- «خط‌مشی امنیت سازمانی» که توسط هدف ارزیابی و محیط عملیاتی‌اش اجرا می‌شود.
- «فرضیاتی» که برای محیط عملیاتی هدف ارزیابی تائید می‌گردند.

- **عامل تهدید (Threat Agent)**

موجودیت‌هایی که می‌توانند بر روی دارایی‌ها اقدام تهاجمی انجام دهند.

1 Security Target

- **خط‌مشی امنیتی سازمانی (OSP[1])**

مجموعه‌ای از قوانین، که توصیف کننده رفتار امنیتی خاصی است که توسط «توابع امنیتی هدف ارزیابی» اجرا می‌گردند؛ این مجموعه قوانین به صورت یک مجموعه از «الزام‌های کارکرد امنیتی» قابل بیان است.

- **اهداف امنیتی (Security Objective)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «اهداف امنیتی» وجود دارد که برای مقابله با تهدیدها معرفی شده و/یا برای برآورده نمودن خط‌مشی‌های امنیت سازمان و یا فرضیات معرفی شده در بخش «مسائل امنیتی»، در نظر گرفته شده است.

- **الزام امنیتی (Security Requirement)**

الزاماتی که به زبان استاندارد بیان می‌شود تا در حاصل شدن اهداف ارزیابی، برای هدف ارزیابی کمک نمایند.

- **الزام کارکرد امنیتی (SFR[2])**

بیان کننده کارکردهای امنیتی هدف ارزیابی در قالب کلاس می‌باشد. در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «الزام کارکرد امنیتی» وجود دارد.

1 Organizational Security Policy
2 Security Functional Requirement

- **الزامات تضمین امنیتی (SAR[1])**

این دسته از الزامات اطمینان می‌دهند که الزامات کارکرد امنیتی توسط هدف ارزیابی برآورده می‌گردند. در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «الزام تضمین امنیتی» وجود دارد.

- **بسته (Package)**

نام مجموعه‌ای از الزامات کارکرد امنیتی یا تضمین امنیتی می‌باشد. به عنوان مثال EAL3.

- **سطح تضمین ارزیابی (EAL[2])**

مجموعه‌ای از الزامات تضمین که از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته شده است و نشان دهنده سطح امنیتی محصول می‌باشد. سطوح تضمین از سطح ۱ تا سطح ۷ می‌باشند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» می‌باشد.

- **توابع امنیتی هدف ارزیابی (TSFs[3])**

آن بخش از هدف ارزیابی که برای اجرای صحیح «الزامات کارکرد امنیتی» باید به آن تکیه نمود، به عنوان «توابع امنیتی هدف ارزیابی» نام برده می‌شود. «توابع امنیتی هدف ارزیابی» شامل تمام سخت‌افزار، نرم‌افزار و میان‌افزارهای هدف ارزیابی است که مستقیم و غیرمستقیم برای اجرا شدن امنیت باید به آنها تکیه نمود.

- **داده توابع امنیتی هدف ارزیابی (TSF data)**

داده‌هایی برای عملیات هدف ارزیابی هستند که اجرای الزامات کارکرد امنیتی وابسته به آنها می‌باشد. این داده‌ها اطلاعات استفاده شده توسط توابع امنیتی هدف ارزیابی هستند.

1 Security Assurance Requirement
2 Evaluation Assurance Level
3 TOE Security Functions

- **داده کاربری (User data)**

داده‌های کاربری هستند که عملکرد توابع امنیتی هدف ارزیابی را تحت تاثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره شده در منابع هدف ارزیابی هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به کار برده می‌شود. محتویات یک پیام الکترونیک نوعی داده کاربری می‌باشد.

- **کلاس (Class)**

مجموعه‌ای از خانواده‌های «استاندارد ارزیابی معیار مشترک» که روی یک موضوع متمرکز، اشتراک دارند.

- **خانواده (Family)**

مجموعه‌ای از عناصر که بر روی یک هدف اشتراک دارند اما در دقت و میزان تاکید، تفاوت دارند.

- **عنصر (Component)[1]**

کوچکترین مجموعه از مؤلفه‌های قابل انتخاب، که الزامات ممکن است براساس آن‌ها باشد.

- **مؤلفه (Element)[2]**

بیانی از نیاز امنیتی که غیر قابل تجزیه است.

- **اختصاص (Assignment)**

مشخص نمودن پارامترهای معرفی شده در یک مؤلفه (از استاندارد معیار مشترک) یا الزام می‌باشد.

---

۱ در استاندارد ملی ISO 15408 منتشر شده توسط سازمان ملی استاندارد، Component مؤلفه ترجمه شده است.

۲ در استاندارد ملی ISO 15408 منتشر شده توسط سازمان ملی استاندارد، Element عنصر ترجمه شده است.

- **انتخاب (Selection)**

انتخاب نمودن یک یا بیش از یک آیتم در لیستی که در مؤلفه یا الزام وجود دارد.

- **سرپرست (Administrator)**

موجودیتی که مسئولیت مدیریت و اعمال خط‌مشی‌ها را بر روی هدف ارزیابی بر عهده دارد و معمولا دارای بالاترین سطح مجوز است.

- **موجودیت فعال (Subject)**

موجودیت فعال، موجودیتی در سیستم مورد ارزیابی (هدف ارزیابی) است که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون سرپرست، کاربر نهایی و غیره. به عبارت دیگر موجودیت فعال عامل انجام عملی بر روی هدف ارزیابی است.

- **موجودیت غیرفعال (Object)**

موجودیت غیرفعال، موجودیتی در سیستم مورد ارزیابی (هدف ارزیابی) می‌باشد که شامل اطلاعات است یا اطلاعات را دریافت می‌کند و روی آن توسط موجودیت‌های فعال، عملیاتی انجام می‌گیرد. همانند داده‌ها و اطلاعاتی همچون متن‌های رمز شده و کلیدها و غیره. به عبارت دیگر موجودیتی است که توسط موجودیت فعال بر روی آن رخدادی اتفاق می‌افتد، مانند لیست کردن رکوردها توسط سرپرست، حذف فایل‌ها توسط حمله کننده، که در این دو مثال رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

- **راز (Secret)**

اطلاعاتی که باید تنها به کاربران مجاز و/یا توابع امنیتی هدف ارزیابی شناسانده شود، تا یک «خط‌مشی کارکرد امنیتی » اجرا شود.

- **مشخصه امنیتی(Security Attribute)**

کاربران، موجودیت‌های فعال، اطلاعات، موجودیت‌های غیرفعال، نشست‌ها و منابع تحت کنترل قوانین «الزامات کارکرد امنیتی» ممکن است دارای اطلاعات خاصی باشند که جهت کارکرد صحیح هدف ارزیابی، مورد استفاده قرار گیرند. دسته‌ای از این اطلاعات حالت آگاهی‌دهنده دارند هم‌چون نام فایل که ممکن است برای معرفی منابع منحصر به فرد استفاده شود، اما دسته‌ی دیگر از این اطلاعات ممکن است به طور خاص برای اجرا شدن الزامات کارکرد امنیتی وجود داشته باشند، همانند اطلاعات کنترل دسترسی، این دسته از اطلاعات به طور کلی «مشخصه امنیتی» نامیده می‌شود.

- **خط‌مشی کارکرد امنیتی(SFP[1])**

رفتار امنیتی که توسط «کارکرد امنیتی هدف ارزیابی» اجرا می‌شود تحت مجموعه قوانینی در «الزامات کارکرد امنیتی» بیان می‌شوند، این مجموعه قوانین «خط مشی کارکرد امنیتی» نامیده می‌شوند. «الزامات کارکرد امنیتی» ممکن است چندین خط‌مشی جهت معرفی قوانینی که هدف ارزیابی باید اجرا کند، تعریف کند. هر کدام از خط‌مشی‌ها باید حوزه کنترلی‌اش را توسط موجودیت‌های فعال، موجودیت‌های غیرفعال، منابع یا اطلاعات و عملکردهایی که بکار برده است، مشخص کند. تمام این خط‌مشی‌ها توسط «توابع امنیتی هدف ارزیابی» پیاده‌سازی می‌شوند.

- **خط‌مشی کارکرد امنیتی کنترل دسترسی (Access Control SFP)**

چندین خط‌مشی کارکرد امنیتی وجود دارد که برای حفاظت از داده‌ها بکار برده می‌شوند، همچون «خط‌مشی کنترل دسترسی» و «خط مشی کنترل جریان اطلاعات». «خط‌مشی کنترل دسترسی» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی کاربران، منابع، موجودیت‌های فعال، موجودیت‌های غیرفعال، نشست‌ها، TSF status data و عملکردها در حوزه کنترلی‌شان پیاده‌سازی می‌شوند.

1 Security Functionality Policy

این مشخصه‌های امنیتی در مجموعه قوانینی استفاده می‌شوند که حاکم بر عملیاتی است که موجودیت‌های فعال ممکن است بر روی موجودیت‌های غیرفعال اجرا نمایند.

- **خط‌مشی کنترل جریان اطلاعات (Information Flow Control SFP)**

«خط‌مشی جریان اطلاعات» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی موجودیت‌های فعال و اطلاعات در حوزه کنترلی‌شان و مجموعه قوانین حاکم بر عملیات که توسط موجودیت فعال بر روی اطلاعات صورت می‌گیرد، پیاده‌سازی می‌شوند.

۳. معرفی استاندارد ۱۵۴۰۸

استاندارد ISO/IEC 15408 که به عنوان استاندارد ارزیابی معیار مشترک[1]نیز شناخته می‌شود با هدف تعیین مبنایی جهت ارزیابی ویژگی‌های امنیتی محصولات فناوری اطلاعات و سیستم‌ها تدوین گردیده است. با ایجاد چنین مبنایی با معیار مشترک، نتایج ارزیابی امنیتی فناوری اطلاعات برای تعداد بیشتری از مخاطبین حائز اهمیت خواهد بود.

استاندارد ISO/IEC 15408 در برگیرنده مؤلفه‌های کارکرد امنیتی بوده که مبنایی برای ارزیابی الزامات کارکرد امنیتی موجود در پروفایل حفاظتی یا سند هدف امنیتی است. این الزامات به توضیح رفتارهای امنیتی مورد نظر هدف ارزیابی[2]یا محیط فناوری اطلاعات پرداخته و هدف آن برآورده نمودن اهداف امنیتی که در پروفایل حفاظتی یا سند هدف امنیتی تعیین شده، می‌باشد.

استاندارد ISO/IEC 15408 در سه بخش ارائه شده است :

بخش اول: مقدمه و مدل عمومی (اصطلاحات و واژگان)

بخش دوم: الزامات کارکرد امنیتی [3]

بخش سوم: الزامات تضمین امنیتی[4]

1 Common Criteria (CC)
2 Target Of Evaluation (TOE)
3 Security Functional Requirement (SFR)
4 Security Assurance Requirement (SAR)

۴. معرفی محصول سوئیچ KVM

این پروفایل حفاظتی، به تجهیزاتی اشاره دارد که به عنوان «سوئیچ به اشتراک گذاری دستگاه‌های جانبی[1]» یا به اختصار «سوئیچ» نامیده می‌شود. که به یک مجموعه از دستگاه‌های «رابط انسانی» اجازه به اشتراک گذاشته شدن بین دو یا بیش از دو کامپیوتر را می‌دهد. هدف ارزیابی معمولاً با تنظیماتی نصب می‌شود که در آن کاربر با یک فضای دستیابی محدود نیاز به دستیابی به دو یا بیش از دو کامپیوتر دارد، که در مجموع «کامپیوترهای سوئیچ شده» نامیده می‌شود (که لازم نیست موجودیت‌های مجزای فیزیکی باشند).

کاربر ممکن است یک صفحه کلید، یک نمایشگر بصری (مانیتور) و یک دستگاه اشاره‌گر (مثل موس) داشته باشد که باید به سوئیچ متصل شود. که در مجموع به عنوان لوازم جانبی مشترک نامیده می‌شود.

در عمل، هدف ارزیابی در هر زمان تنها به یک کامپیوتر متصل می‌شود. برای استفاده از کامپیوترهای مختلف، کاربر باید اعمال خاصی را انجام دهد (فشار یک دکمه، دستگیره و ...). هدف ارزیابی، سپس کامپیوتری که توسط کاربر انتخاب شده است را نمایش می‌دهد. هدف ارزیابی باید مانع هرگونه ویژگی شود که سبب اجازه دادن به اطلاعات کاربری جهت به اشتراک گذارده شدن یا منتقل شدن بین کامپیوترها از طریق هدف ارزیابی می‌گردند.

«گروه پورت جانبی» مجموعه‌ای از پورت‌های دستگاه است که به عنوان یک موجودیت تنها توسط هدف ارزیابی عمل می‌کند. یک گروه برای مجموعه‌ای از تجهیزات جانبی به اشتراک گذارده شده و یک گروه برای هر کامپیوتر متصل سوئیچ شده وجود دارد. هر گروه کامپیوتر سوئیچ شده دارای یک شناسه ID منحصر به فرد است. شناسه گروه تجهیزات جانبی به اشتراک گذارده شده، مشابه گروه کامپیوتر سوئیچ شده که اخیراً توسط هدف ارزیابی انتخاب شده است، می‌باشد.

1 Peripheral Sharing switch (PSS)

خط مشی کارکرد امنیتی داده‌های مجزا[1]

هدف ارزیابی باید به داده‌های جانبی اجازه دهد که تنها بین گروه‌های پورت جانبی با ID مشابه منتقل شوند.

خود هدف ارزیابی، جریان اطلاعات کاربری بین تجهیزات به اشتراک گذاشته شده و کامپیوترهای سوئیچ شده را در نظر نمی‌گیرد. هدف ارزیابی تنها یک اتصال بین تجهیزات واسط انسانی و «کامپیوتر انتخاب شده» در هر لحظه ارائه می‌دهد.

این نوع سوئیچ‌ها، ممکن است نسبت به پرینتر "A/B" خودی یا سوئیچ‌های پورت سریال تفاوت معنا داری داشته باشند، که در آن بدون محدودیت بر روی اتصال بین دستگاه‌ها قرار می‌گیرند.

برخی سوئیچ‌ها ممکن است دارای ویژگی‌های بیشتری هم‌چون، اسکن نمودن (که در آن به طور مستمر بین کامپیوترها سوئیچ می‌کند تا زمانی‌که اقدام به متوقف نمودن سوئیچ کند) یا پروتکل ویدئو که اطلاعات ترکیبی در محیط کامپیوتر را تبدیل می‌نمایند، باشند. این روند باید مورد بررسی قرار گیرد تا مطمئن شویم که اطلاعات بین کامپیوترها به اشتراک گذاشته نشده یا منتقل نگردیده است.

1 Data Separation Security Function Policy (SFP)

۵. تعریف مسائل امنیتی

۱.۵ خط‌مشی

A.TYPE	توضیحات
A.ACCESS	یک کاربر مجاز، مجوزهای لازم را جهت دسترسی به اطلاعاتی که توسط هدف ارزیابی انتقال داده شده است دارا باشد.
A. MANAGE	هدف ارزیابی مطابق با راهنمایی‌های سازنده، نصب و مدیریت شود.
A. NOEVIL	کاربر مجاز متخاصم نیست و از تمامی راهنمایی‌های کاربردی استفاده می‌کند.
A. PHYSICAL	هدف ارزیابی از نظر فیزیکی امن است.

۲.۵ تهدیدها

T.TYPE	توضیحات
T.INVALIDUSB	کاربر مجاز، دستگاه‌های USB غیرمجاز را به سوئیچ KVM متصل کند.
T.RESIDUAL	داده‌های رسوب کرده (داده‌های جانبی ذخیره شده در یک سوئیچ) ممکن است بین گروه‌های پورت جانبی با IDهای متفاوت منتقل شوند.
T.ROM_PROG	توابع امنیتی هدف ارزیابی ممکن است توسط یک هکر ویرایش شوند.
T.SPOOF	توسط فعالیت‌های عمدی یا سهوی ممکن است یک کاربر اینطور فکر کند که مجموعه‌ای از دستگاه‌های جانبی به اشتراک گذاشته شده به یک کامپیوتر مشخص متصل شده‌اند، در حالی‌که در حقیقت به کامپیوتر دیگری وصل شده‌اند.
T.TRANSFER	یک ارتباط بین کامپیوترها ممکن است توسط هدف ارزیابی، اجازه انتقال اطلاعات داشته باشد.

۶. اهداف امنیتی

۱.۶ اهداف امنیتی هدف ارزیابی

O.TYPE	توضیحات
O.CONF	هدف ارزیابی نباید محرمانگی اطلاعاتی را که پردازش می‌کند، نقض کند. اطلاعات تولید شده در داخل هر ارتباط کامپیوتر گروه دستگاه‌های جانبی، نباید توسط هیچ گروه دستگاه جانبی دیگری از طریق ID گروه متفاوت قابل دسترسی باشد.
O.INDICATE	کاربر مجاز باید یک علامت واضح و غیر مبهم از کامپیوتر سوئیچ شده‌ای که انتخاب شده است دریافت کند.
O.ROM	نرم‌افزار و سخت‌افزار هدف ارزیابی باید در مقابل تغیرات و ویرایش‌های غیرمجاز محافظت شده باشد. نرم‌افزار جایگذاری شده در هدف ارزیابی باید شامل حافظه‌ای از نوع ROM باشد که با پوشش محافظ برنامه‌ریزی شده یا تنها یکبار قابل برنامه‌ریزی باشد، که بصورت دائمی (و نه سوکتی) به یک اجتماع مدار متصل شده است.
O.SELECT	یک فعالیت آشکار توسط کاربر مجاز باید برای انتخاب کامپیوتر مورد نظر جهت اتصال به مجموعه‌ای از دستگاه‌های به اشتراک گذاشته شده که به یکدیگر متصل شده‌اند استفاده شود که با دکمه فشاری تکی یا دکمه فشاری چندگانه یا انتخاب روش‌های چرخشی که توسط بیشتر محصولات تجاری امروزی مورد استفاده قرار می‌گیرند انجام می‌شود. سوئیچینگ

O.TYPE	توضیحات
	اتوماتیکی که بر مبنای اسکن کردن می‌باشد نباید به عنوان یک مکانیزم انتخاب، استفاده شود.
O.SWITCH	تمامی دستگاه‌های موجود در گروه دستگاه‌های جانبی به اشتراک گذاری شده باید در هر لحظه حداکثر به یک کامپیوتر سوئیچ شده متصل شوند.
O.USBDETECT	هدف ارزیابی باید هر نوع اتصال USB را که از نوع قلم نوری، موس، صفحه‌کلید یا صفحه نمایش باشد کشف کند و پس از شناسایی اولیه هیچ عمل متقابلی را در مورد ابزارهای مذکور انجام ندهد.

۲.۶ اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
OE.ACCESS	کاربر مجاز باید مجوزهای لازم جهت دسترسی به اطلاعاتی را که توسط هدف ارزیابی منتقل می‌شوند داشته باشد.
OE.MANAGE	هدف ارزیابی باید مطابق با راهنمایی‌های سازنده، نصب و مدیریت شود.

OE.TYPE	توضیحات
OE.NOEVIL	کاربر مجاز نباید متخاصم باشد و باید از تمامی راهنمایی‌های کاربردی استفاده کند.
OE.PHYSICAL	هدف ارزیابی باید از نظر فیزیکی امن باشد.

۷. الزامات کارکرد امنیتی

۱.۷ کلاس حفاظت از داده‌های کاربری

در ادامه المان‌های امنیتی مورد نیاز حوزه حفاظت از داده‌های کاربری ارائه شده است.

نام کلاس: حفاظت از داده کاربری

شرح کلاس: این کلاس شامل خانواده‌هایی است که الزامات مربوط به محافظت از داده کاربر را مشخص می‌نمایند: خانواده‌های محافظت از داده کاربر در چهار گروه زیر دسته بندی شده‌اند، که علاوه بر مشخصه‌های امنیتی مربوط به داده کاربری، داده‌های کاربری در داخل هدف ارزیابی را در طول ورود، خروج و ذخیره سازی نیز آدرس‌دهی می‌کنند.

خانواده‌های این کلاس در چهار گروه زیر دسته بندی شده‌اند:

۱) خط‌مشی‌های امنیتی مربوط به محافظت از داده کاربری

- خط‌مشی‌های کنترل دسترسی (حف-س‌ک)[1]
- خط‌مشی‌های مرتبط با کنترل جریان اطلاعات (حف-خج)[2]

در این دو خانواده، به نویسنده هدف امنیتی/پروفایل حفاظتی اجازه داده می‌شود تا خط‌مشی‌های امنیتی که برای حفاظت از داده‌کاربری در نظر گرفته شده و همچنین حوزه کنترلی این خط‌مشی‌ها نام برده شود.

خط‌مشی‌های امنیتی نام برده شده در این دو خانواده عبارتند از :

- خط‌مشی‌های امنیتی در نظر گرفته شده برای کنترل دسترسی

1 Access control policy(FDP_ACC)
2 Information flow control policy(FDP_IFC)

- خط‌مشی‌های امنیتی در نظر گرفته شده برای کنترل جریان اطلاعات

توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش «انتخاب» یا «اختصاص» فراخوانی می‌گردند.

در دو خانواده توابع کنترل دسترسی (ح‌ف-ت‌ک)[۱] و توابع کنترل جریان اطلاعات (ح‌ف-ک‌ج)[۲] قوانینی که تعریف کننده « خط‌مشی‌های امنیتی کنترل دسترسی» و « خط‌مشی‌های امنیتی کنترل جریان اطلاعات» هستند، آورده شده است.

۲) فرم‌های مختلف محافظت از داده کاربری

- توابع کنترل دسترسی (ح‌ف-ت‌ک)
- توابع کنترل جریان اطلاعات (ح‌ف-ک‌ج)
- انتقال داخلی در هدف ارزیابی (ح‌ف-اد)[۳]
- حفاظت از اطلاعات باقیمانده (ح‌ف-اب)[۴]
- عملیات عقب‌گرد به منظور بازگرداندن حالت/حالت‌های قبل (ح‌ف-ع‌گ)[۵]
- یکپارچگی داده‌های ذخیره شده (ح‌ف-ی‌د)[۶]

۳) ورود و خروج، ذخیره‌سازی برون‌خطی[۷]

1 Access control functions(FDP_ACF)
2 Information flow control functions(FDP_IFF)
3 Internal TOE transfer(FDP_ITT)
4 Residual information protection(FDP_RIP)
5 Rollback(FDP_ROL)
6 Stored data integrity(FDP_SDI)
7 Offline

- احراز هویت[1] داده (حف-تد)
- صادر شده از هدف ارزیابی (حف-صا)[2]
- ورود داده‌ها از بیرون به هدف ارزیابی (حف-وب)[3]

مؤلفه‌های این خانواده، انتقال قابل اعتماد به داخل یا خارج از هدف ارزیابی را آدرس‌دهی می‌کنند.

۴) ارتباطات میان توابع امنیتی هدف ارزیابی

- محافظت از انتقال محرمانگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-مد)[4]
- محافظت از انتقال یکپارچگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-یا)[5]

مؤلفه‌های این خانواده ارتباطات بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن فناوری اطلاعات را آدرس‌دهی می‌کند.

➢ خانواده خط‌مشی‌های کنترل دسترسی

این خانواده خط‌مشی‌های امنیتی مربوط به کنترل دسترسی را نام می‌برد و حوزه کنترلی سیاست‌گذاری‌ها را تعریف می‌کند. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال[6] تحت کنترل سیاست‌گذاری‌ها
- موجودیت‌های غیرفعال[1] تحت کنترل سیاست‌گذاری‌ها

1 Data authentication(FDP_DAU)
2 Export from the TOE(FDP_ETC)
3 Import from outside of the TOE(FDP_ITC)
4 Inter-TSF user data confidentiality transfer protection(FDP_UCT)
5 Inter-TSF user data integrity transfer protection(FDP_UIT)
6 Subject

- عملیات بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده که توسط خط‌مشی‌های امنیتی پوشش داده می‌شود.

بنابراین در مؤلفه‌های این خانواده، خط‌مشی امنیتی نامبرده می‌شود و برای هریک از خط‌مشی‌های امنیتی نامبرده شده، موجودیت فعال و غیرفعال تحت کنترل آن خط‌مشی و عملیات بین موجودیت فعال و غیرفعال نیز نامبرده می‌شود.

در این خانواده می‌توان خط‌مشی‌های امنیتی مختلفی برای کنترل دسترسی داشت و هریک نام منحصر به فرد خود را داشته باشند تنها باید مؤلفه‌های این خانواده برای هر یک از خط‌مشی‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال ح‌ف-س‌ک.۱٫۱(۱)، ح‌ف-س‌ک.۱٫۱(۲)).

قوانینی که عملکرد خط‌مشی‌های امنیتی را برای کنترل دسترسی تعریف می‌نمایند، در خانواده‌های توابع کنترل دسترسی (ح‌ف-ت‌ک) و صادر شده از هدف ارزیابی (ح‌ف-ص‌ا) تعریف می‌شوند.

خط‌مشی‌های نام برده شده در این خانواده توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش «انتخاب» یا «اختصاص» فراخوانی می‌گردند.

➢ خانواده توابع کنترل دسترسی

در خانواده خط‌مشی‌های امنیتی کنترلی دسترسی (ح‌ف-س‌ک)، تنها این خط‌مشی‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای خط‌مشی امنیتی بر روی عملیات بین موجودیت‌های فعال و غیرفعال (نام برده شده در خانواده (ح‌ف-س‌ک)) وضع می‌شود. هم‌چنین در این خانواده موجودیت‌های فعال و غیرفعال تحت کنترل خط-مشی‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نامبرده می‌شوند.

---

1 Object

- **خانواده احراز هویت داده**

احراز هویت داده به هر نهادی، اجازه پذیرش مسوولیت احراز صحت اطلاعات را می‌دهد (با دیجیتالی امضاء نمودن اطلاعات). این خانواده روشی را مشروط بر تضمین اعتبار یک بخش خاص از داده ارائه می‌کند که می‌تواند به منظور بررسی محتوای اطلاعات از لحاظ جعل نشدن یا تغییر یافتن مکرر مورد استفاده قرار گیرد.

- **خانواده صادرشده از هدف ارزیابی**

در دو خانواده (حف-س‌ک) و (حف-خج) خط‌مشی‌های امنیتی بر روی کنترل دسترسی و جریان اطلاعات نامبرده شده‌اند. در این خانواده این خط‌مشی‌های امنیتی بر روی داده تحت کنترل این خط‌مشی‌ها هنگام خروج از هدف ارزیابی اعمال می‌شود، مشخصه‌های امنیتی داده‌ها هنگام صدور می‌تواند حفظ گردیده یا نادیده گرفته شود. در واقع در این خانواده محدودیت‌هایی برای صدور داده از هدف ارزیابی اعمال می‌شود.

- **خط‌مشی‌های کنترل جریان اطلاعات**

این خانواده سیاست‌گذاری‌های عملکرد امنیتی مربوط به کنترل جریان اطلاعات را نام می‌برد و برای هریک از آنها، حوزه کنترلی را تعریف می‌کند. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال تحت کنترل سیاست‌گذاری‌ها
- اطلاعات تحت کنترل سیاست‌گذاری‌ها
- عملیاتی که سبب کنترل اطلاعات جریان یافته به/از موجودیت‌های فعال کنترل شده تحت پوشش این خط‌مشی‌ها می‌باشند.

بنابراین در مؤلفه‌های این خانواده، خط‌مشی امنیتی نامبرده می‌شوند و برای هریک از خط‌مشی‌های امنیتی نامبرده شده، موجودیت فعال و غیرفعال تحت کنترل آن خط‌مشی و عملیات بین موجودیت فعال و غیرفعال نیز نامبرده می‌شوند.

در این خانواده می‌توان خط‌مشی‌های امنیتی مختلفی برای کنترل دسترسی داشت و هریک نام منحصر به فرد خود را داشته باشند تنها باید مؤلفه‌های این خانواده برای هر یک از خط‌مشی‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-خج.۱,۱(۱)، حف-خج.۱,۱(۲)).

قوانینی که عملکرد خط‌مشی‌های امنیتی را برای کنترل دسترسی تعریف می‌نمایند، در خانواده‌های توابع کنترل دسترسی (حف-کج) و صادر شده از هدف ارزیابی (حف-ص-ا) تعریف می‌شوند.

خط‌مشی‌های نام برده شده در این خانواده توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش «انتخاب» یا «اختصاص» فراخوانی می‌گردند.

- **خانواده توابع کنترل جریان اطلاعات**

در خانواده خط‌مشی‌های امنیتی کنترلی دسترسی (حف-خج)، تنها این خط‌مشی‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای خط‌مشی امنیتی بر روی عملیات بین موجودیت‌های فعال و غیرفعال (نام برده شده در خانواده (حف-خج)) وضع می‌شود. هم‌چنین در این خانواده موجودیت‌های فعال و غیرفعال تحت کنترل خط‌مشی‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نامبرده می‌شوند. این خانواده شامل دو الزام است:

- یکی پرداختن به مسائل عملکرد جریان اطلاعات رایج
- پرداختن به جریان اطلاعات غیرمجاز

این تقسیم‌بندی به این دلیل مطرح شده است که مسائل مربوط به جریان اطلاعات غیرمجاز، در برخی موارد با باقی سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات در تعامد است. با توجه به طبیعتشان سرپیچی نمودن آنها از سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات، منجر به نقص در خط‌مشی‌ها می‌شود. بنابراین، باید عملیات‌های خاصی برای جلوگیری یا محدود نمودن جریان اطلاعات غیرمجاز در نظر گرفت.

- **خانواده ورود داده‌ها از بیرون به هدف ارزیابی**

این خانواده تعریف کننده سازوکارهایی برای ورود داده‌های کاربری تحت کنترل خط‌مشی‌های امنیتی (خط‌مشی‌های امنیتی کنترل جریان و کنترل دسترسی) از خارج هدف ارزیابی می‌باشد. برای ورود داده باید خط‌مشی‌های تعریف شده بر روی داده اعمال شود، هم‌چنین مشخصه‌های امنیتی مطلوبی برای اینگونه از داده‌ها در نظر گرفته می‌شود. در واقع این خانواده محدودیت‌هایی بر روی داده‌های ورودی از خارج هدف ارزیابی اعمال می‌کند.

- **خانواده انتقال هدف ارزیابی داخلی**

این خانواده الزاماتی را ارائه می‌دهد تا از داده کاربری در زمانی‌که بین بخش‌های مجزای هدف ارزیابی در سراسر کانال داخلی [1]انتقال می‌یابد، حفاظت کند. هم‌چنین در این خانواده داده‌ها را براساس مشخصه‌های امنیتی از یکدیگر مجزا نموده و برای شناسایی خطا در صحت داده، داده‌های منتقل شده بین بخش‌های هدف ارزیابی مانیتور می-گردند.

- **خانواده حفاظت از اطلاعات باقیمانده**

این خانواده اطمینان می‌دهد در زمانی‌که منبع از یک موجودیت غیرفعال آزاد می‌شود و دوباره به یک موجودیت غیرفعال دیگر اختصاص داده می‌شود، هرگونه داده موجود در منابع، در دسترس قرار نمی‌گیرد. این خانواده نیاز دارد که از هرگونه داده موجود در منابع که به طور منطقی حذف یا آزاد می‌شود، محافظت کند، اما ممکن است هنوز در داخل منابع کنترل شده توابع امنیتی هدف ارزیابی اطلاعاتی وجود داشته باشد که به موجودیت غیرفعال دیگری اختصاص داده شود.

1 Internal channel

- **خانواده عملیات عقب‌گرد به منظور بازگرداندن حالت/ حالت‌های قبل**

عملکرد عقب‌گرد شامل بی‌اثر نمودن آخرین عملکرد یا یک سری از عملکردها، محدود شدن به برخی محدودیت‌ها هم‌چون بازه زمانی و برگشت به یک وضعیت شناخته شده قبلی می‌باشد. عقب‌گرد فراهم کننده قابلیت بی‌اثر نمودن عملیات یا مجموعه‌ای از عملیات است تا یکپارچگی داده کاربری را حفظ کند.

- **خانواده صحت داده‌های ذخیره شده**

این خانواده الزاماتی را ارائه می‌کند که از داده کاربری ذخیره شده در کانتینر تحت کنترل توابع امنیتی هدف ارزیابی، محافظت می‌کند. خطای صحت ممکن است داده کاربری ذخیره شده در حافظه یا در یک ابزار ذخیره‌سازی را تحت تاثیر قرار بدهند. این خانواده صحت داده‌های ذخیره شده را حفظ می‌کند و ممکن است در صورت تشخیص خطا، اقدامی در برابر آن انجام بدهد، اما خانواده «انتقال هدف ارزیابی داخلی (حف-اد)» صحت داده کاربری در حال انتقال در هدف ارزیابی را محافظت می‌کند.

- **خانواده محافظت از انتقال محرمانگی داده کاربر در توابع امنیتی هدف ارزیابی داخلی**

این خانواده تعریف کننده الزاماتی است که محرمانگی داده کاربری را در زمانی‌که با استفاده از یک کانال خارجی بین هدف ارزیابی و دیگر محصولات امن IT انتقال می‌یابد، تضمین می‌کند.

- **خانواده محافظت از انتقال صحیح داده کاربر در داخلی عملکرد امنیتی هدف ارزیابی**

این خانواده الزاماتی را تعریف می‌کند تا صحت داده کاربری را که بین هدف ارزیابی و دیگر محصولات امن IT منتقل می‌شود، تامین کند و از داده کاربری را از خطاهای قابل تشخیص بازیابی کند. این خانواده حداقل داده کاربری را جهت اطمینان از تغییر نیافتن مانیتور می‌کند. همچنین، این خانواده از روش‌های مختلف جهت اصلاح خطاهای تشخیص داده شده در صحت داده پشتیبانی می‌کند.

شماره الزام	نام خانواده	عنصر امنیتی
۱	خط مشی مرتبط با کنترل جریان اطلاعات (FDP_IFC)	**نام عنصر: خط مشی مرتبط با کنترل جریان اطلاعات (زیر مجموعه کنترل جریان اطلاعات) ۱** **شماره مؤلفه: ح‌ف-خ‌ج.۱,۱(FDP_IFC.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید خط مشی عملکرد امنیتی مجزا سازی داده را بر روی مجموعه‌ای از گروه پورت‌های دستگاه جانبی اجرا نمایند و داده‌های جانبی بین دستگاه‌های جانبی مشترک و کامپیوترهای سوئیچ شده به صورت دو طرفه جریان یابند.
۲	عملیات کنترل جریان اطلاعات (FDP_IFF)	**نام عنصر: عملیات کنترل جریان اطلاعات (صفات امنیتی ساده) ۱** **شماره مؤلفه: ح‌ف-ک‌ج.۱,۱(FDP_IFF.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید خط مشی عملکرد امنیتی مجزا سازی داده را براساس انواع موجودیت‌های فعال زیر و صفات امنیت اطلاعات اجرا نمایند: گروه‌های پورت دستگاه جانبی (موجودیت فعال)، داده دستگاه جانبی و شناسه گروه پورت دستگاه جانبی (صفات)

شماره الزام	نام خانواده	عنصر امنیتی
۳		**نام عنصر: عملیات کنترل جریان اطلاعات (صفات امنیتی ساده) ۱** **شماره مؤلفه: ح‌ف-ک‌ج.۲,۱(FDP_IFF.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید اجازه جریان اطلاعات بین یک موجودیت فعال کنترل شده و اطلاعات کنترل شده را از طریق عملکرد کنترل شده بدهند، چنان‌چه دارای قوانین زیر باشند: قوانین سوئیچینگ: داده جانبی می‌تواند به یک گروه پورت جانبی با یک شناسه جریان یابد، تنها به شرطی‌که از یک گروه پورت جانبی با همان شناسه دریافت شده باشد.
۴		**نام عنصر: عملیات کنترل جریان اطلاعات (صفات امنیتی ساده) ۱** **شماره مؤلفه: ح‌ف-ک‌ج.۳,۱(FDP_IFF.1.3)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید [هیچ قوانین خط مشی عملکرد امنیتی کنترل جریان اطلاعات اضافی] را اجرا کنند.

شماره الزام	نام خانواده عنصر امنیتی
۵	**نام عنصر: عملیات کنترل جریان اطلاعات (صفات امنیتی ساده) ۱** **شماره مؤلفه: ح‌ف-ک‌ج.۴,۱(FDP_IFF.1.4)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید موارد زیر را ارائه دهند: [هیچ یک از قابلیت‌های خط مشی عملکرد امنیتی کنترل جریان اطلاعات اضافی]
۶	**نام عنصر: عملیات کنترل جریان اطلاعات (صفات امنیتی ساده) ۱** **شماره مؤلفه: ح‌ف-ک‌ج.۵,۱(FDP_IFF.1.5)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به صراحت اجازه جریان یافتن اطلاعات براساس قوانین زیر را بدهند: [بدون هیچ قوانین اضافی]
۷	**نام عنصر: عملیات کنترل جریان اطلاعات (صفات امنیتی ساده) ۱** **شماره مؤلفه: ح‌ف-ک‌ج.۶,۱(FDP_IFF.1.6)** **شرح مؤلفه:**

شماره	نام خانواده
الزام	عنصر امنیتی

توابع امنیتی هدف ارزیابی باید به صراحت جریان اطلاعات براساس قوانین زیر را انکار نمایند:

[بدون هیچ قانون اضافی]

۲.۷ کلاس مدیریت امنیت

هدف ارزیابی نیازی به نقش مدیریتی مجزا ندارد. با این حال نیاز است که قابلیتی ارائه شود تا جنبه‌های خاصی از هدف ارزیابی که نباید در دسترس کاربر معمول قرار بگیرد را پیکربندی کند. اگر هدف ارزیابی، سطحی از کنترل سرپرستی را ارائه دهد، بنابراین الزام مناسب توسط پیوست الف باید در هدف امنیتی استفاده شود.

نام کلاس: مدیریت امنیت

شرح کلاس: این کلاس جهت مشخص نمودن مدیریت ویژگی‌های مختلف توابع امنیتی هدف ارزیابی در نظر گرفته شده است. در این کلاس مشخصه‌های امنیتی، توابع و داده‌های توابع امنیتی هدف ارزیابی، نقش‌های مدیریتی مختلف و تعاملاتشان، هم‌چون جداسازی قابلیت‌ها ، می‌توانند مشخص گردند.

این کلاس دارای چندین هدف است:

- مدیریت داده توابع امنیتی هدف ارزیابی برای مثال علامت‌ها[1]
- مدیریت مشخصه‌های امنیتی، برای مثال لیست‌های کنترل دسترسی و لیست قابلیت‌ها
- مدیریت کارکرد توابع امنیتی هدف ارزیابی برای مثال، انتخاب توابع ، نقش‌ها یا شرایطی که رفتار توابع امنیتی هدف ارزیابی را تحت تاثیر قرار می‌دهند.
- تعریف نقش‌های امنیتی

[1] Banner

خانواده‌های آن در ادامه آمده است.

- **خانواده مدیریت کارکرد توابع امنیتی هدف ارزیابی[1]**

این خانواده اجازه کنترل کاربران مجاز در حین مدیریت کارکرد توابع امنیتی هدف ارزیابی را می‌دهد. مثالی از عملکردها در توابع امنیتی هدف ارزیابی شامل ممیزی توابع و توابع احراز هویت چندگانه می‌باشد.

- **خانواده مدیریت مشخصه‌های امنیتی[2]**

این خانواده اجازه کنترل کاربران مجاز در حین مدیریت مجوزهای امنیتی را می‌دهد. این مدیریت می‌تواند شامل قابلیتی برای مشاهده و تغییر مجوزهای امنیتی باشد.

- **خانواده مدیریت داده‌های توابع امنیتی هدف ارزیابی[3]**

این خانواده اجازه کنترل کاربران (نقش‌ها) مجاز در حین مدیریت داده‌های توابع امنیتی هدف ارزیابی را می‌دهد. مثالی از داده توابع امنیتی هدف ارزیابی می‌تواند شامل ممیزی اطلاعات، ساعت و دیگر پارامترهای پیکربندی توابع امنیتی هدف ارزیابی باشد.

- **خانواده لغو[4]**

این خانواده لغو مشخصه‌های امنیتی انواع موجودیت‌ها در هدف ارزیابی را آدرس‌دهی می‌کند.

[1] Management of functions in TSF (FMT_MOF)
[2] Management of security attributes (FMT_MSA)
[3] Management of TSF data (FMT_MTD)
[4] Revocation (FMT_REV)

- **خانواده انقضای مشخصه امنیتی[1]**

این خانواده قادر به اعمال محدودیت زمانی برای اعتبار مشخصه‌های امنیتی می‌باشد.

- **خانواده مشخصات کارکردهای مدیریت[2]**

این خانواده اجازه می‌دهد تا مشخصات عملکردهای مدیریتی توسط هدف ارزیابی ایجاد شوند. عملکردهای مدیریتی با استفاده از ایجاد رابط توابع امنیتی هدف ارزیابی، به سرپرستان اجازه می‌دهند تا پارامترهایی برای کنترل عملکرد ویژگی‌های مربوط به امنیت هدف ارزیابی تعریف کند، مانند مجوزها و صفات حفاظت از داده، مجوزها و صفات حفاظت از هدف ارزیابی، مجوزها و صفات ممیزی و مجوزها و صفات شناسایی و احراز هویت.

عملکردهای مدیریتی هم‌چنین شامل آن دسته از عملکردهایی است که توسط کاربر اجرا می‌شود تا تداوم عملکرد هدف ارزیابی را تضمین کند، مانند عملکردهای پشتیبانی و بازیابی. عملکرد این خانواده بر روی دیگر مؤلفه‌ها در کلاس مدیریت امنیت تاثیر دارد.

- **خانواده نقش‌های مدیریت امنیتی[3]**

این خانواده برای کنترل اختصاص نقش‌های مختلف به کاربران در نظرگرفته شده است. توانایی این نقش‌ها با توجه به مدیریت امنیتی است که در دیگر خانواده‌های این کلاس توصیف شده است.

1 Security attribute expiration (FMT_SAE)
2 Specification of Management Functions (FMT_SMF)
3 Security management roles (FMT_SMR)

شماره الزام	نام خانواده	عنصر امنیتی
۸	مدیریت مشخصه‌های امنیتی (FMT_MSA)	**نام عنصر: مدیریت رفتار توابع امنیتی (مدیریت صفات امنیتی) ۱** **شماره مؤلفه: م‌د-م‌ا.۱,۱.۱ (FMT_MSA.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید خط مشی عملکرد امنیتی مجزا سازی داده را اجرا کند تا توانایی تغییر صفات امنیتی شناسه‌های گروه پورت‌های جانبی را به کاربر محدود کند. نکته کاربردی: کاربر مجاز باید در یک اقدام صریح، کامپیوتری را که مجموعه‌ای از دستگاه‌های جانبی متصل شده را به اشتراک گذاشته است را انتخاب کند، بنابراین می‌توان شناسه گروه مربوط به دستگاه‌های جانبی را تغییر داد.
۹		**نام عنصر: مدیریت رفتار توابع امنیتی (مقداردهی اولیه صفات استاتیک) ۳** **شماره مؤلفه: م‌د-م‌ا.۱,۳.۱ (FMT_MSA.3.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید «خط مشی کارکرد امنیتی مجزاسازی داده» را اجرا کند تا بتواند مقادیر

شماره الزام	نام خانواده	عنصر امنیتی

پیش‌فرض محدودی را برای صفات امنیتی ارائه کند، که در اجرای خط مشی کارکرد امنیتی» مورد استفاده قرار می‌گیرند.

نکته کاربردی:

هنگام راه‌اندازی، فقط و فقط باید یک کامپیوتر متصل شده انتخاب شود.

۱۰ **نام عنصر: مدیریت رفتار توابع امنیتی (مقداردهی اولیه صفات استاتیک) ۳**

شماره مؤلفه: م‌د-م‌ا.۲,۳.۱ (FMT_MSA.3.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید به **هیچ** اجازه دهد تا مقادیر اولیه جایگزین را مشخص کند تا زمانی‌که یک موجودیت غیرفعال یا اطلاعاتی ایجاد می‌شود، مقادیر پیش فرض را نادیده بگیرد.

۳.۷ الزامات توسعه یافته

شماره الزام	نام خانواده	عنصر امنیتی
۱۱	قانون شاخص بصری (EXT_VIR)	**نام عنصر: قانون شاخص بصری ۱** **شماره مؤلفه: ت‌س-ش‌ب.۱،۱ (EXT_VIR.1.1)** **شرح مؤلفه:** روش بصری نشان خواهد داد که کامپیوتر به مجموعه‌ای مشترک از دستگاه‌های جانبی متصل خواهد شد، به شرطی‌که به طور مداوم برای مدت زمانی متصل باشد. **نکته کاربردی:** نیازی به شاخص‌های لمسی نمی‌باشد، اما وجود آنها بلامانع است.
۱۲	اتصال USB نامعتبر (EXT_IUC)	**نام عنصر: اتصال USB نامعتبر ۱** **شماره مؤلفه: ت‌س-ان.۱،۱ (EXT_IUC.1.1)** **شرح مؤلفه:** تمام دستگاه‌های USB، که به سوئیچ‌های جانبی متصل به سوئیچ‌های جانبی باید مورد استنطاق قرار

شماره الزام	نام خانواده	عنصر امنیتی
		بگیرند تا از معتبر بودن آنها اطمینان حاصل شود (دستگاه اشاره‌گر، صفحه کلید، نمایشگر). تعامل بیشتر با دستگاه‌های غیر معتبر نباید انجام گیرد.
۱۳	حافظه فقط خواندنی (EXT_ROM)	**نام عنصر: حافظه فقط خواندنی ۱** **شماره مؤلفه: ت‌س-ح‌خ.۱,۱.۱ (EXT_ROM.1.1)** **شرح مؤلفه:** نرم‌افزار توابع امنیتی هدف ارزیابی جاسازی شده در حافظه فقط خواندنی توابع امنیتی هدف ارزیابی باید در ماسک برنامه‌ریزی شده یا حافظه فقط خواندنی که فقط یکبار قابل برنامه‌ریزی است به صورت دائمی به مدار مونتاژ شده متصل شود.

۸. الزامات تضمین امنیتی

نام کلاس	نام عنصر (component)	توضیحات
Development	ADV_FSP.2	مشخصات کارکرد ابتدایی
	ADV_ARC.1	معماری امنیتی
	ADV_TDS.1	طراحی اولیه
Guidance Documents	AGD_OPE.1	راهنمای کاربری عملیاتی
	AGD_PRE.1	راهنمای کاربری آماده‌سازی
Tests	ATE_IND.2	آزمون مستقل- انطباق
	ATE_FUN.1	آزمون کارکردی
	ATE_COV.1	مدارک پوشش
Vulnerability Assessment	AVA_VAN.2	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.2	استفاده از سیستم پیکربندی
	ALC_CMS.2	قسمت‌هایی از پوشش مدیریت پیکربندی هدف ارزیابی
	ALC_DEL.1	رویه‌های تحویل

نام کلاس	نام عنصر (component)	توضیحات
	ALC_FLR.2	رویه‌های گزارش‌دهی نقص

۱.۸ کلاس توسعه

۱.۱.۸ خانواده معماری امنیتی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۱	توصیف معماری امنیتی (ADV_ARC)	**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.1D)** **شرح مؤلفه:** توسعه دهنده باید هدف ارزیابی را طوری پیاده‌سازی و طراحی کند که نتوان ویژگی‌های امنیتی توابع امنیتی هدف ارزیابی را دور زد.
۲		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_ARC.1.2D)**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: توسعه دهنده باید طوری توابع امنیتی هدف ارزیابی را طراحی و پیاده‌سازی کند تا بتواند از خود در برابر مداخله توسط موجودیت‌های فعال ناامن، محافظت کند.
۳		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_ARC.1.3D)** **شرح مؤلفه:** توسعه دهنده باید توصیفی از معماری امنیتی توابع امنیتی هدف ارزیابی ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۴	توصیف معماری امنیتی **(ADV_ARC)**	**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.1C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		سند معماری امنیتی باید سطح جزئیاتش متناسب با توصیف واسط اجرا کننده کارکرد امنیتی باشد که در سند طراحی هدف ارزیابی ذکر شده است.
۵		**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.2C)** **شرح مؤلفه:** سند معماری امنیتی باید دامنه امنیتی نگهداری شده توسط توابع امنیتی هدف ارزیابی سازگار با الزامات کارکرد امنیتی را توصیف کند.
۶		**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.3C)** **شرح مؤلفه:** توصیف معماری امنیتی باید شرح دهد که فرآیند مقداردهی اولیه توابع امنیتی هدف ارزیابی چگونه امن شده است.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۷		**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.4C)** **شرح مؤلفه:** سند معماری امنیتی باید نشان دهد که توابع امنیتی هدف ارزیابی از خود در برابر مداخله محافظت می‌نمایند.
۸		**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.5C)** **شرح مؤلفه:** سند معماری امنیتی باید نشان دهد، توابع امنیتی هدف ارزیابی از دور زدن عملکرد واسط اجرا کننده کارکرد امنیتی جلوگیری می‌نمایند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۹	توصیف معماری امنیتی **(ADV_ARC)**	**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند.

۲.۱.۸ خانواده مشخصات کارکردی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۰	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.1D)** **شرح مؤلفه:** توسعه دهنده باید مشخصات کارکردی را ارائه کند.

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۱۱		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.2D)** **شرح مؤلفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۱۲	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.1C)** **شرح مؤلفه:** مشخصات کارکردی باید توابع امنیتی هدف ارزیابی را به طور کامل نمایش دهد.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۱۳		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.2C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و روش‌های مورد استفاده برای تمام واسط‌های توابع امنیتی هدف ارزیابی را توصیف کند.
۱۴		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.3C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مربوط به هر واسط توابع امنیتی هدف ارزیابی را معرفی و توصیف کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۱۵		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.4C)** **شرح مؤلفه:** برای هر واسط اجرا کننده کارکرد امنیتی، مشخصات کارکردی باید اقدامات آن واسط را توصیف نمایند.
۱۶		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.5C)** **شرح مؤلفه:** برای واسط اجرا کننده کارکرد امنیتی، سند مشخصات کارکردی باید پیغام خطاهایی را توصیف کند که مستقیماً از پردازش اقدامات اجراکننده کارکرد امنیتی ناشی شده‌اند.
۱۷		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.6C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		ردیابی‌ها باید نشان دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌ها در سند مشخصات کارکردی باشند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۱۸	مشخصات کارکردی (ADV_FSP)	**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند.
۱۹		**نام عنصر: مشخصات کارکردی واسط اجرا کننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		ارزیاب باید مشخص کند که سند مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

۳.۱.۸ خانواده طراحی هدف ارزیابی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۲۰	طراحی هدف ارزیابی (ADV_TDS)	**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.1D)** **شرح مؤلفه:** توسعه دهنده باید طراحی هدف ارزیابی را ارائه کند.
۲۱		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.2D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		توسعه دهنده باید نگاشتی از واسطهای سند مشخصات کارکردی به پائین‌ترین سطح از اجزای طراحی هدف ارزیابی ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۲۲	طراحی هدف ارزیابی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.1C)** **شرح مؤلفه:** طراحی باید ساختار هدف ارزیابی را به صورت زیرمجموعه‌ای توصیف کند.
۲۳		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.2C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		سند طراحی باید تمام زیرمجموعه‌های توابع امنیتی هدف ارزیابی را معرفی کند.
۲۴		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.3C)** **شرح مؤلفه:** سند طراحی باید رفتار هر زیرمجموعه پشتیبان کننده الزام کارکرد امنیتی و غیر مداخله کننده الزام کارکرد امنیتی را با جزئیات کافی شرح داده و نشان دهد که زیرمجموعه اجراکننده کارکرد امنیتی نمی‌باشند.
۲۵		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.4C)** **شرح مؤلفه:** طراحی باید به طور خلاصه رفتار اجرا کننده کارکرد امنیتی از زیرمجموعه‌های اجراکننده کارکرد امنیتی را بیان کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۲۶		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.5C)** **شرح مؤلفه:** طراحی باید شرحی از تعاملات بین زیرمجموعه‌های اجرا کننده کارکرد امنیتی و هم‌چنین بین این زیرمجموعه‌ها و دیگر زیرمجموعه‌ها بیان دارد.
۲۷		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.6C)** **شرح مؤلفه:** نگاشت باید نشان دهد که تمام رفتاری که در سند طراحی توصیف شده است به واسطهای درخواست کننده آنها نگاشت شده‌اند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۸	طراحی هدف ارزیابی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.
۲۹	طراحی هدف ارزیابی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.2E)** **شرح مؤلفه:** ارزیاب باید تعیین کند که طراحی، نمونه‌ای دقیق و کامل از تمام الزامات کارکرد امنیتی است.

۲.۸ کلاس مستندات راهنما

۱.۲.۸ خانواده راهنمای کاربری عملیاتی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۳۰	راهنمای کاربردی (AGD_OPE)	**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۳۱	راهنمای کاربردی (AGD_OPE)	**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی که باید در یک

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		محیط پردازشی امن کنترل شوند را توصیف کند، همانند هشدارهای مناسب.
۳۲		**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف کند که چگونه از واسطهای در دسترس ارائه شده توسط هدف ارزیابی به صورت امن استفاده می‌شود.
۳۳		**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسطهای دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۳۴		**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویداد مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط کند، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی هدف ارزیابی.
۳۵		**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مودهای عملیاتی هدف ارزیابی (مودهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۳۶		**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی که توسط کاربر تبعیت می‌شوند را توصیف کند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده است، کاملاً اجرا گردند.
۳۷		**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۳۸	راهنمای کاربردی (AGD_OPE)	**نام عنصر: راهنمای کاربری عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۲.۲.۸ خانواده راهنمای کاربری آماده‌سازی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۳۹	راهنمای آماده‌سازی (AGD_PRE)	**نام عنصر: راهنمای کاربری آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:** توسعه دهنده باید هدف ارزیابی را همراه با سند آماده‌سازی ارائه کند.

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

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

۳.۸ کلاس آزمون

۱.۳.۸ خانواده آزمون پوشش

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۴۴	آزمون پوشش (ATE_COV)	**نام عنصر: آزمون پوشش ۱** **شماره مؤلفه: (ATE_COV.1.1D)** **شرح مؤلفه:** توسعه دهنده باید مدارک آزمون پوشش را ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۴۵	آزمون پوشش (ATE_COV)	**نام عنصر: آزمون پوشش ۱** **شماره مؤلفه: (ATE_COV.1.1C)** **شرح مؤلفه:** مدارک ارائه شده برای آزمون پوشش باید نشان‌دهنده ارتباط بین آزمون‌های سند آزمون و واسط‌های

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		توابع امنیتی هدف ارزیابی در سند مشخصات کارکردی باشند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۴۶	آزمون پوشش **(ATE_COV)**	**نام عنصر: آزمون پوشش ۱** **شماره مؤلفه: (ATE_COV.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۲.۳.۸ خانواده آزمون کارکردی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۴۷	آزمون کارکردی (ATE_FUN)	**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.1D)** **شرح مؤلفه:** توسعه دهنده باید توابع امنیتی هدف ارزیابی را بیازماید و نتایج آن را مستند کند.
۴۸		**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.2D)** **شرح مؤلفه:** توسعه دهنده باید سند آزمون را ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۴۹	آزمون کارکردی	**نام عنصر: آزمون کارکردی ۱**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
	(ATE_FUN)	**شماره مؤلفه: (ATE_FUN.1.1C)** **شرح مؤلفه:** سند آزمون باید شامل طرح آزمون، نتایج مورد انتظار آزمون و نتایج واقعی آزمون باشد.
۵۰		**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.2C)** **شرح مؤلفه:** طرح آزمون باید آزمون‌های صورت گرفته را معرفی و سناریوی انجام هر آزمون را توصیف کند. این سناریو همچنین باید شامل ترتیب وابستگی به نتایج دیگرآزمون‌ها باشد.
۵۱		**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.3C)** **شرح مؤلفه:** نتایج آزمون مورد انتظار آزمون، باید خروجی مورد انتظار از اجرای موفق آزمون را نشان دهد.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۲		**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.4C)** **شرح مؤلفه:** نتایج واقعی آزمون باید با نتایج مورد انتظار آزمون سازگار باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۳	آزمون کارکردی **(ATE_FUN)**	**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند.

۳.۳.۸ خانواده آزمون مستقل

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۵۴	آزمون مستقل **(ATE_IND)**	**نام عنصر: نمونه آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.1D)** **شرح مؤلفه:** توسعه دهنده باید برای آزمودن، هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۵۵	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.1C)** **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۶		**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.2C)** **شرح مؤلفه:** توسعه دهنده باید معادل مجموعه منابعی که در آزمون کارکردی توسعه دهنده استفاده شده‌اند را برای ارزیاب فراهم کند.

مؤلفه‌های اقدامات ارزیاب		
۵۷	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند.
۵۸		**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.2E)**

مؤلفه‌های اقدامات ارزیاب		
		شرح مؤلفه: ارزیاب باید نمونه‌ای از آزمون‌ها در سند آزمون را اجرا کند تا از نتایج آزمون توسعه دهنده اطمینان حاصل کند.
۵۹		**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.3E)** **شرح مؤلفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی هدف ارزیابی را بیازماید تا اطمینان حاصل کند که توابع امنیتی هدف ارزیابی به صورت مشخص شده عمل می‌کند.

۴.۸ کلاس ارزیابی آسیب‌پذیری

۱.۴.۸ خانواده تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۶۰	تحلیل آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: تحلیل آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.1D)** **شرح مؤلفه:** توسعه دهنده باید برای آزمودن، هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۶۱	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: تحلیل آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.1C)** **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۶۲	آسیب‌پذیری (AVA_VAN)	**نام عنصر: تحلیل آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌کند.
۶۳		**نام عنصر: تحلیل آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در هدف ارزیابی، در منابع عمومی جستجویی را انجام دهد.
۶۴		**نام عنصر: تحلیل آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.3E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		ارزیاب باید آنالیز آسیب‌پذیری هدف ارزیابی را با استفاده از مستندات راهنما، سند مشخصات کارکردی، طراحی هدف ارزیابی و توصیف معماری امنیتی انجام دهد تا آسیب‌پذیری‌های بالقوه در هدف ارزیابی را معرفی کند.
۶۵		**نام عنصر: تحلیل آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.4E)** **شرح مؤلفه:** ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ را انجام دهد تا مقاومت هدف ارزیابی در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرندرا مشخص کند.

۵,۸کلاس پشتیبانی از چرخه حیات

۱.۵.۸ خانواده قابلیت‌های مدیریت پیکربندی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۶۶	قابلیت‌های مدیریت پیکربندی (ALC_CMC)	**نام عنصر: استفاده از یک سیستم مدیریت پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.1D)** **شرح مؤلفه:** توسعه دهنده باید هدف ارزیابی و مرجع هدف ارزیابی را ارائه کند.
۶۷		**نام عنصر: استفاده از یک سیستم مدیریت پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.2D)** **شرح مؤلفه:** توسعه دهنده باید سند پیکربندی را ارائه کند.
۶۸		**نام عنصر: استفاده از یک سیستم مدیریت پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.3D)**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: توسعه دهنده باید از یک سیستم پیکربندی استفاده کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۶۹	قابلیت‌های مدیریت پیکربندی **(ALC_CMC)**	**نام عنصر: استفاده از یک سیستم مدیریت پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.1C)** **شرح مؤلفه:** هدف ارزیابی باید با یک مرجع یکتا برچسب زده شود.
۷۰		**نام عنصر: استفاده از یک سیستم مدیریت پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.2C)** **شرح مؤلفه:** مستندات پیکربندی باید روش مورد استفاده برای معرفی یکتای موارد پیکربندی را معرفی کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۷۱		**نام عنصر: استفاده از یک سیستم مدیریت پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.3C)** **شرح مؤلفه:** سیستم پیکربندی باید تمام موارد پیکربندی را به صورت یکتا معرفی کند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۷۲	قابلیت‌های مدیریت پیکربندی **(ALC_CMC)**	**نام عنصر: استفاده از یک سیستم مدیریت پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۲.۵.۸ خانواده حوزه مدیریت پیکربندی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۳	حوزه مدیریت پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش مدیریت پیکربندی بخشی از هدف ارزیابی ۲** **شماره مؤلفه: (ALC_CMS.2.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۴	حوزه مدیریت پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش مدیریت پیکربندی بخشی از هدف ارزیابی ۲** **شماره مؤلفه: (ALC_CMS.2.1C)** **شرح مؤلفه:** لیست پیکربندی باید شامل خود هدف ارزیابی، مدارک مورد نیاز توسط الزامات تضمین امنیتی و بخش-هایی که شامل هدف ارزیابی هستند، باشد.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۷۵		**نام عنصر: پوشش مدیریت پیکربندی بخشی از هدف ارزیابی ۲** **شماره مؤلفه: (ALC_CMS.2.2C)** **شرح مؤلفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی کند.
۷۶		**نام عنصر: پوشش مدیریت پیکربندی بخشی از هدف ارزیابی ۲** **شماره مؤلفه: (ALC_CMS.2.3C)** **شرح مؤلفه:** برای هر یک از موارد پیکربندی مربوط به توابع امنیتی هدف ارزیابی، لیست پیکربندی باید توسعه دهنده آن را نشان دهد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۷۷	حوزه مدیریت پیکربندی	**نام عنصر: پوشش مدیریت پیکربندی بخشی از هدف ارزیابی ۱**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
	(ALC_CMS)	**شماره مؤلفه: (ALC_CMS.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۳.۵.۸ خانواده تحویل

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۷۸	تحویل (ALC_DEL)	**نام عنصر: رویه‌های تحویل ۱** **شماره مؤلفه: (ALC_DEL.1.1D)** **شرح مؤلفه:** توسعه دهنده باید رویه تحویل هدف ارزیابی یا بخشی از آن را به مشتری، مستند کند.
۷۹		**نام عنصر: رویه تحویل ۱** **شماره مؤلفه: (ALC_DEL.1.2D)**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: توسعه دهنده باید از رویه‌های تحویل استفاده کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۸۰	تحویل (ALC_DEL)	**نام عنصر: رویه تحویل ۱** **شماره مؤلفه: (ALC_DEL.1.1C)** **شرح مؤلفه:** مستندات تحویل باید تمام رویه‌هایی که برای حفظ امنیت در زمان توزیع نسخه‌های هدف ارزیابی لازم و ضروری هستند را شرح دهد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۸۱	تحویل (ALC_DEL)	**نام عنصر: رویه تحویل ۱** **شماره مؤلفه: (ALC_DEL.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۴.۵.۸ خانواده اصلاح نقص

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۸۲	اصلاح نقص (ALC_FLR)	**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.1D)** **شرح مؤلفه:** توسعه دهنده باید رویه‌های اصلاح نقص که به توسعه دهنده هدف ارزیابی داده می‌شوند را مستند کند.

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۸۳		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.2D)** **شرح مؤلفه:** توسعه دهنده باید رویه‌ای برای پذیرش تمام گزارشات نقص امنیتی و اقدام نمودن بر روی آنها، هم-چنین درخواست تصحیح نقص را ایجاد کند.
۸۴		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.3D)** **شرح مؤلفه:** توسعه دهنده باید راهنمای اصلاح نقص را به کاربران هدف ارزیابی ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۸۵	اصلاح نقص (ALC_FLR)	**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.1C)** **شرح مؤلفه:** مستندات رویه‌های اصلاح نقص باید رویه‌هایی را توصیف نمایند که در هر هدف ارزیابی منتشر شده برای پیگیری نقص‌های امنیتی گزارش شده مورد استفاده قرار می‌گیرند.
۸۶		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.2C)** **شرح مؤلفه:** رویه‌های اصلاح نقص باید ملزم به توصیف ماهیت و اثر هر نقص امنیتی ارائه شده، هم‌چنین وضعیت اصلاحیه یافته شده برای آن نقص باشند.
۸۷		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.3C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		رویه‌های اصلاح نقص باید ملزم به معرفی اقدامات اصلاحی برای هر نقص امنیتی باشند.
۸۸		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.4C)** **شرح مؤلفه:** مستندات رویه‌های اصلاح نقص باید روش‌هایی را توصیف نمایند که به کاربران هدف ارزیابی، اطلاعات نقص، اصلاحیه‌ها و راهنمایی در رابطه با اقدامات اصلاحی ارائه می‌دهند.
۸۹		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.5C)** **شرح مؤلفه:** رویه‌های اصلاح نقص باید امکانی را فراهم کنند تا توسعه دهنده بتواند گزارش‌ها و درخواست‌های مربوط به نقص‌های امنیتی مشکوک در هدف ارزیابی را از کاربران آن دریافت کند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۹۰		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.6C)** **شرح مؤلفه:** رویه پردازش نقص امنیتی گزارش شده، باید اطمینان دهد که هر نقص گزارش شده اصلاح می‌شود وهم‌چنین رویه اصلاح به کاربر هدف ارزیابی داده می‌شود.
۹۱		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.7C)** **شرح مؤلفه:** رویه پردازش نقص امنیتی گزارش شده، باید هرگونه اصلاح نقص امنیتی را از مطرح نمودن نقص جدید در هدف ارزیابی حفاظت کند.
۹۲		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.8C)**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: راهنمای اصلاح نقص باید امکانی را فراهم کند که کاربران هدف ارزیابی بتوانند هرگونه نقص امنیتی مشکوک در هدف ارزیابی را به توسعه دهنده گزارش دهند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۹۳	اصلاح نقص **(ALC_FLR)**	**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.