به نام خدا

پروفایل حفاظتی
یکسو کننده جریان داده

اردیبهشت ۹۶

نسخه ۱,۰

با تشکر و سپاس از همکاری

صنایع الکترونیک زعیم

فهرست

۱ مقدمه

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده نمودن الزامات ارائه شده‌اند در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهند کرد. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را بر اساس سند نظام ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 در راستای این هدف تهیه کرده است. این پروفایل حفاظتی به بیان الزامات یکسو کننده جریان داده که هیچ‌گونه کنسول مدیریتی ندارد می‌پردازد.

۲ شرح محصول

مخاطرات مختلفی شبکه‌های محلی سازمان‌ها را تهدید می‌کنند که این موجب شده است تا سازمان‌ها شبکه‌های ایزوله از هم داشته باشند: به عنوان مثال می‌توان به جدا بودن شبکه اینترنت از شبکه سازمان اشاره کرد. با وجود جدا بودن این شبکه‌ها، نیاز به انتقال اطلاعات بین شبکه‌ها وجود دارد. معمولاً نیازمندی اصلی انتقال اطلاعات از یک شبکه به شبکه دیگر –و نه برعکس– است.

اتصال شبکه‌های ایزوله می‌تواند با ابزارهای مختلفی انجام شود: یکی از این ابزارها یکسو کننده جریان داده است. این محصول به صورت کاملاً سخت‌افزاری ارتباطی یک‌طرفه بین دو شبکه برقرار می‌نماید این ارتباط از طریق کانالی سخت‌افزاری برقرار می‌شود که تمام سیگنال‌های در خلاف جهت از بین می‌روند و سیگنال فقط از یک طرف به طرف دیگر حرکت می‌کند و این ارتباط کاملاً به صورت سخت‌افزاری یک‌طرفه شده است. شکل ۱ نمایی از این محصول و قرارگیری آن در معماری شبکه را مشاهده می‌نمایید.

این پروفایل حفاظتی برای آن دسته از محصولات یکسو کننده جریان داده انتشار شده است که هیچ‌گونه کنسول مدیریتی برای پیکربندی محصول فراهم نمی‌کند. از این رو برای سایر محصولاتی که ارائه‌کننده کنسول مدیریتی هستند باید علاوه بر الزامات مطرح شده در این پروفایل، الزامات موجود در پروفایل حفاظتی تجهیز شبکه یا دیگر الزامات تعیین شده در پروفایل‌های آتی نیز برآورده نمایند.

شکل ۱: معماری سطح بالا از Data Diode

این محصول خط‌مشی ارسال یک‌طرفه داده را پیاده‌سازی نموده است که در زیر توصیف می‌شود:

- موجودیت‌های فعال:
  - پورت پایین/ارسال‌کننده (واسط ورودی یکسو کننده جریان داده)
  - پورت بالا/دریافت‌کننده (واسط خروجی یکسو کننده جریان داده)
- اطلاعات (سیگنال‌هایی که می‌توانند در خروجی بالا و یا خروجی پایین ورود نمایند)
- خط‌مشی
  - اطلاعات فقط اجازه دارند از پورت پایین وارد شده و از پورت بالا خارج شوند.
  - اطلاعات اجازه ندارند از پورت بالا وارد شده و از پورت پایین خارج شوند.

۳ مسائل امنیتی

۱,۳ تهدیدات محیطی

تهدید[۱] اقدام مخربی[۲] است که توسط عامل تهدید[۳] روی یک دارایی[۴] انجام می‌شود. اقدام مخرب، اعمالی هستند که توسط عامل تهدید روی یک دارایی انجام می‌شود. این اقدامات برخی خاصیت‌های یک دارایی را تحت تأثیر قرار می‌دهند که ارزش[۵] آن دارایی از آن‌هاست. عامل تهدید می‌تواند در قالب نوع و یا گروهی از تهدیدها توصیف شود. در جدول ۱ زیر دارایی را نشان می‌دهد و جدول ۲ و ۳ به ترتیب تهدیدات بر روی عامل‌ها و تهدیدات نشت اطلاعات را نشان می‌دهد.

جدول ۱: دارایی

دارایی‌ها	توضیحات
اطلاعات سطح بالا HIGHINFO	هر اطلاعات سطح بالا در سمت گیرنده به عنوان اطلاعات حساس خوانده می‌شود.

جدول ۲: تهدیدات عامل‌ها

عامل تهدید	توضیحات
عامل پایین TA-LOW	هر سیستمی که به شبکه سطح پایین (فرستنده) متصل است یا حمله‌کننده‌ای که به این سیستم متصل باشد. سیستم سطح پایین ممکن است از تنوع و تعداد زیادی از ابزارها و وسایلی گوناگونی که بتوانند سیستم را مورد تهدید قرار دهند تشکیل شده باشد.
عامل بالا TA-HIGH	هر سیستمی که به شبکه سطح بالا (گیرنده) متصل است یا حمله‌کننده‌ای که به این سیستم متصل است. سیستم سطح بالا ممکن است از تنوع و تعداد زیادی از ابزارها و وسایلی گوناگونی که بتوانند سیستم را مورد تهدید قرار دهند تشکیل شده باشد.

[۱] threat
[۲] Adverse Action
[۳] Threat agent
[۴] Asset
[۵] Value

جدول ۳: تهدیدات

تهدیدات	توضیحات
نشت اطلاعات T.DATA_LEAK	هرکدام از سیستم‌های ارسال‌کننده و دریافت‌کننده می‌تواند باعث نشت و درز اطلاعات شود.

۲,۳ خط‌مشی امنیتی

خط‌مشی‌ها	توضیحات
ارتباط یک‌طرفه P.ONE_WAY_FLOW	تمام ارتباطات باید از یک طرف «ارسال‌کننده» و از طرف دیگر «دریافت‌کننده» دریافت شود.

۳,۳ فرضیات

فرضیات	توضیحات
فیزیکی A.PHYSICAL	محصول و پورت‌های ارتباطی آن به صورت فیزیکی در مقابل دسترسی غیرمجاز و هر مداخله فیزیکی، مانند مداخله‌های مکانیکی، الکتریکی، اپتیکی، تشعشعی محافظت می‌شوند.
نصاب آموزش‌دیده A.INTEGRATOR	فرض شده است کسی که عملیات نصب و پیکربندی محصول را انجام می‌دهد (نصاب) این کار را به صورت صحیح، بر طبق راهنمای کاربری انجام می‌دهد و به‌جز محصول راه ارتباطی دیگری بین دو شبکه قرار نمی‌دهد.

۴ اهداف امنیتی

۱,۴ اهداف امنیتی برای محصول

هدف	توضیحات
محرمانگی O.NO_HIGH_INFO	تمام اطلاعات سمت گیرنده باید به صورت محرمانه نسبت به طرف ارسال‌کننده باشد و هیچ اطلاعاتی نباید به سمت ارسال‌کننده از طرف گیرنده فرستاده شود.
ارسال یک‌طرفه O.ONE_WAY_FLOW	تمام اطلاعات از سمت ارسال‌کننده به سمت گیرنده ارسال می‌شود.

۲,۴ اهداف امنیتی برای محیط عملیاتی

هدف	توضیحات
فیزیکی OE.PHYSICAL	محصول و پورت‌های ارتباطی آن به صورت فیزیکی در مقابل دسترسی غیرمجاز و هر مداخله فیزیکی، مانند مداخله‌های مکانیکی، الکتریکی، اپتیکی، تشعشعی محافظت می‌شوند.
نصاب آموزش‌دیده OE.INETGRATOR	فرض شده است کسی که عملیات نصب و پیکربندی محصول را انجام می‌دهد (نصاب) این کار را به صورت صحیح، بر طبق راهنمای کاربری انجام می‌دهد و به‌جز محصول راه ارتباطی دیگری بین دو شبکه قرار نمی‌دهد.

۵ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با **Error! Reference source not found.**زیر هستند و در ادامه هریک از الزامات شرح و بسط داده شده‌اند. الزامات تشریح شده در این بخش الزامی هستند و تمامی محصولات باید آن‌ها را رعایت نمایند.

شماره الزام	نام الزام	عنصر متناظر با الزام
۱	خط‌مشی کنترل جریان اطلاعات ۲	FDP_IFC.2.1
۲	خط‌مشی کنترل جریان اطلاعات ۳	FDP_IFC.2.2
۳	عملیات کنترل جریان اطلاعات ۱	FDP_IFF.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۴	عملیات کنترل جریان اطلاعات 2	FDP_IFF.1.2
۵	عملیات کنترل جریان اطلاعات 3	FDP_IFF.1.3
۶	عملیات کنترل جریان اطلاعات 4	FDP_IFF.1.4
۷	عملیات کنترل جریان اطلاعات 5	FDP_IFF.1.5

۱,۵ کلاس حفاظت از داده کاربری

شماره الزام	نام الزام
۱	**خط‌مشی کنترل جریان اطلاعات ۲**
محصول باید **خط‌مشی ارسال یک‌طرفه** را روی **موجودیت‌های فعال: پورت‌های بالا و پایین/اطلاعات: هر نوع سیگنال نوری که از پورت بالا یا پایین عبور کند** و هر نوع عملیاتی که منجر به عبور اطلاعات از/به موجودیت‌های فعال تحت این خط‌مشی شود اعمال کند.	
۲	**خط‌مشی کنترل جریان اطلاعات ۳**
محصول اطمینان می‌دهند که همه عملیاتی که ردوبدل شدن اطلاعات در موجودیت‌های فعال محصول را در برمی‌گیرند توسط یک خط‌مشی[۶] پوشش داده می‌شود.	
۳	**عملیات کنترل جریان اطلاعات ۱**
محصول باید **خط‌مشی ارسال یک‌طرفه** را بر اساس این نوع مشخصه‌های امنیتی اطلاعات و موجودیت‌های فعال اعمال کند: **موجودیت‌های فعال: پورت‌های بالا و پایین – اطلاعات: هر نوع سیگنال نوری که از پورت بالا یا پایین عبور کند.**	

[۶] SFP

نکته کاربردی ۱: هیچ مشخصه‌ای برای موجودیت‌های فعال بیان نشده است. هر نوع اطلاعاتی که در بالا بیان شده است با این الزامات کارکرد امنیتی پوشش داده می‌شود.	
۴	**عملیات کنترل جریان اطلاعات 2**
با توجه به قوانین زیر، محصول باید اجازه جریان یافتن اطلاعات بین یک موجودیت فعال کنترل‌شده و اطلاعات کنترل‌شده را از طریق عملیات کنترل‌شده بدهد: [اختصاص: برای هر عملیات، باید ارتباطی بر اساس مشخصه امنیتی بین اطلاعات و موجودیت فعال وجود داشته باشد.]	
۵	**عملیات کنترل جریان اطلاعات 3**
محصول باید [اختصاص: قوانین بیشتر برای خط‌مشی کنترل جریان اطلاعات] اعمال نماید.	
۶	**عملیات کنترل جریان اطلاعات 4**
محصول باید بر اساس قوانین زیر اجازه‌ی جریان یافتن اطلاعات را دهد: [اختصاص: قوانین مبتنی بر مشخصه‌های امنیتی که به‌صورت صریح جریان اطلاعات را مجاز می‌نمایند.]	
۷	**عملیات کنترل جریان اطلاعات 5**
محصول باید بر اساس قوانین زیر مانع جریان یافتن اطلاعات شود: [اختصاص: قوانین مبتنی بر مشخصه‌های امنیتی که صراحتاً از جریان یافتن اطلاعات جلوگیری می‌نماید.]	

۶ الزامات تضمین امنیت

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی محصول است. در این بخش الزامات EAL1 آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۱,۶ کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نیست، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه‌دهندگان محصول باشد.

۲,۶ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

دستورالعمل نصب موفقیت‌آمیز محصول در محیط

دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگ‌تر

دستورالعمل‌هایی که ارائه‌دهنده قابلیت مدیریتی محافظت‌شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۱,۲,۷ راهنمای کاربری

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شماره مؤلفه: (AGD_OPE.1.4C) **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی	**نام عنصر: راهنمای کاربردی ۱**

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

2.2.7راهنمای آماده‌سازی

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده-سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

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

۳,۶ کلاس آزمون

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

۱,۳,۷ آزمون مستقل

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

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

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

مؤلفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آزمون مستقل ۱ **شماره مؤلفه: (ATE_IND.1.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب	
	ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را آزمون نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.

۴,۶ کلاس آسیب‌پذیری

۱,۴,۷ تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
	ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۵,۶ کلاس پشتیبانی از چرخه حیات

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

۱,۵,۷ قابلیت‌های پیکربندی

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

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول و مرجع محصول را ارائه نماید.

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

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

۲,۵,۷ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

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

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

۷ پیوست یک: اصطلاحات

Security Target (ST)	هدف امنیتی
Conformance Claim	ادعای انطباق
High Side	سمت بالا (گیرنده)
Low Side	سمت پایین (فرستنده)
High Port	پورت بالا (پورت گیرنده)
Low Port	پورت پایین (پورت فرستنده)
Physical Scope	حوزه فیزیکی
Logical Scope	حوزه منطقی
Security Problem Definition	مسائل امنیتی
Assets	دارایی‌ها
Threat Agent	عامل تهدید
Threats	تهدیدات
Assumptions	فرضیات
Organizational Security Policies	خط‌مشی امنیتی
Security Objectives	اهداف امنیتی
Security Objectives for the Operational Environment	اهداف امنیتی برای محیط عملیاتی
Security Objectives Rationale	منطق اهداف امنیتی
Coverage	پوشش
Sufficiency	کفایت
Security Requirements	الزامات امنیتی
One-way Security Functional Requirement (SFR)	خط‌مشی ارسال یک‌طرفه
Security Functional Requirements (SFR)	الزامات کارکرد امنیتی
Target of Evaluation (TOE)	محصول
Complete information flow control	کنترل جریان اطلاعات کامل
Information	اطلاعات
Subjects	موجودیت‌های فعال
Objects	موجودیت‌های غیرفعال
Simple security attributes	مشخصه‌های امنیتی ساده

Security Requirements Rationale	منطق نیازمندی‌های امنیتی
Security Assurance Requirements	الزامات تضمین امنیت
Security Assurance Requirements Rationale	منطق الزامات تضمین امنیتی
Evaluation Assurance Level (EAL)	سطح تضمین امنیتی
TOE Security Functions (TSF)	محصول