گزارش عدم انطباق‌های مشاهده شده در آزمون ارزیابی امنیتی

سیستم یکپارچه شهرسازی آمارد–فاز اول

(قابل ارائه به مشتری)

کنترل کننده: مهری یحیائی تأییدکننده: مهری یحیائی تاریخ و امضاء: ۱۴۰۱/۱۰/۰۸	تاریخ انتشار: ۱۴۰۱/۱۰/۰۸ ویرایش: ۱.۰
آزمایشگاه آزمون: مرکز تحقیقات صنایع انفورماتیک	آدرس: خیابان کریم‌خان‌زند، خیابان شهیدعضدی جنوبی، نبش رودسر، پلاک ۳ تلفن: ۹۸۲۱۸۸۹۲۵۹۵۰+ فکس: ۹۸۲۱۸۸۹۳۷۶۵۸+
مشتری: تحلیل گران آمارد نوین	آدرس: مازندران– آمل– بلوار آزادگان– نبش آزادگان ۵۲– ساختمان آمارد تلفن: ۰۱۱۴۳۲۷۰۹۴۱ فکس: داخلی۵
نام و شماره استاندارد مرجع آزمون:	1- ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security, Common Criteria Apr 2017, Version 3.1, Revision 5 , Part: 1,2,3 2- Application Security Verification Standard Version 2014 (ASVS 2014)
ویژگی محصول مورد آزمون: نام سامانه : نرم افزار یکپارچه شهرسازی آمارد علامت تجاری: آمارد مدل: تحت وب نسخه نرم‌افزار: 1401.03.21.01 تولید کننده محصول: تحلیل گران آمارد نوین	شماره سند هدف امنیتی[1] محصول: نسخه ۱.۶ تاریخ انتشار سند هدف امنیتی محصول: مردادماه– ۱۴۰۱ نویسنده سند هدف امنیتی محصول: شرکت تحلیل گران آمارد نوین
مرجع سند پروفایل حفاظتی[2] مورد آزمون: پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه، مرکز مدیریت راهبردی افتا، نسخه ۱.۱ تاریخ انتشار سند پروفایل حفاظتی محصول: اسفند ۹۶ سایر مراجع: ASVS 2014	محل مهر محرمانه این سند در ۴۹ صفحه تنظیم شده است.

[1] Security Target
[2] Protection Profile

فهرست مطالب

فهرست جداول

این سند براساس الزامات سطح ۱ استاندارد ASVS و همچنین آخرین نسخه استاندارد ISO/IEC 15408 و متدولوژی CEM تهیه شده و الزامات سطح EAL1 را پوشش می‌دهد.

جدول ۱ : عنوان سه بخش استاندارد ISO/IEC 15408

Applicable Common Criteria Version Apr 2017, Version 3.1, Revision 5	
Common Criteria for Information Technology Security Evaluation Part 1	Introduction and general model
Common Criteria for Information Technology Security Evaluation Part 2	Security functional components
Common Criteria for Information Technology Security Evaluation Part 3	Security assurance components

جدول ۲ : متدولوژی CEM

Common Evaluation Methodology Version Apr 2017, Version 3.1, Revision 5	
Common Methodology for Information Technology Security Evaluation	Evaluation methodology

جدول ۳ : استاندارد ASVS

ASVS August 2014, Version 2.0	
Application Security Verification Standard	web application security verification

۱- مقدمه

در گزارش حاضر **فاز اول** از نتایج ارزیابی محصول سیستم یکپارچه شهرسازی آمارد منعکس شده‌است. موارد زیر مورد ارزیابی قرار گرفته است:

- الزامات کارکردی امنیت بر اساس پروفایل حفاظتی برنامه کاربردی تحت شبکه
- الزامات تضمین امنیت سطح ۱ (EAL1)

توجه:

- نتایج حاصل از ارزیابی آسیب پذیری محصول مورد آزمون بر اساس استاندارد ASVS متعاقباً و در **فاز دوم** ارایه خواهد شد.

۱-۱- مشخصات محصول

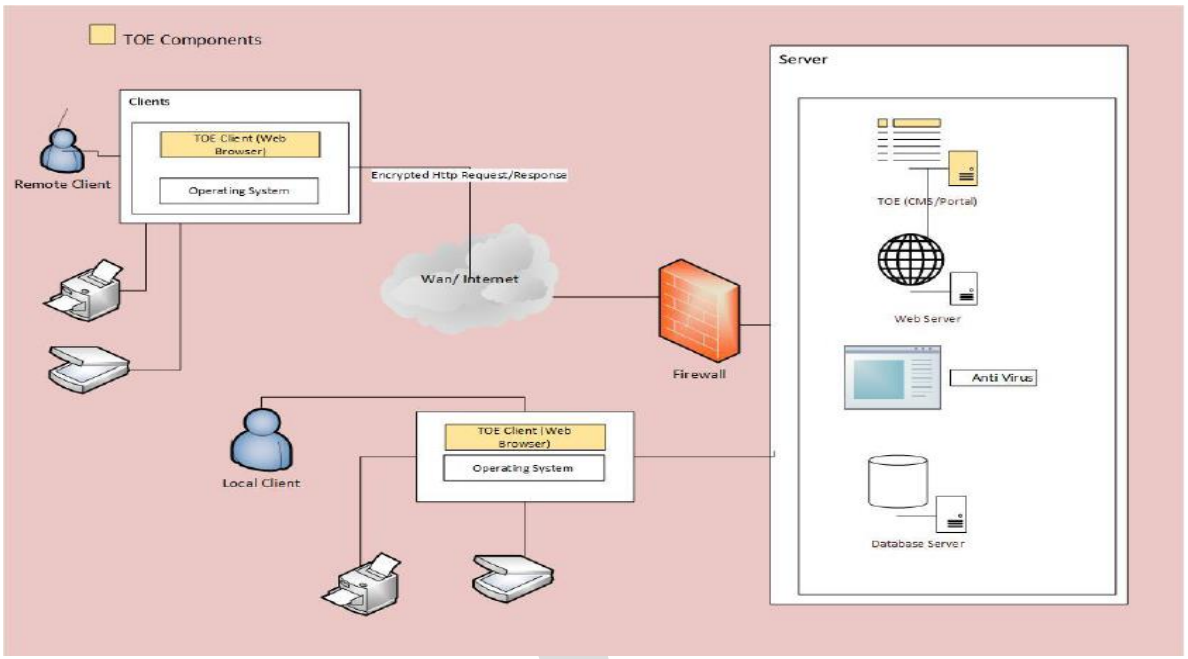
از جمله قابلیت‌های محصول که در سند مشخصات فنی و ویژگی‌های سیستم بیان شده است می‌توان به موارد زیر اشاره کرد:

جدول ۱-۱: مشخصات محصول مورد آزمون

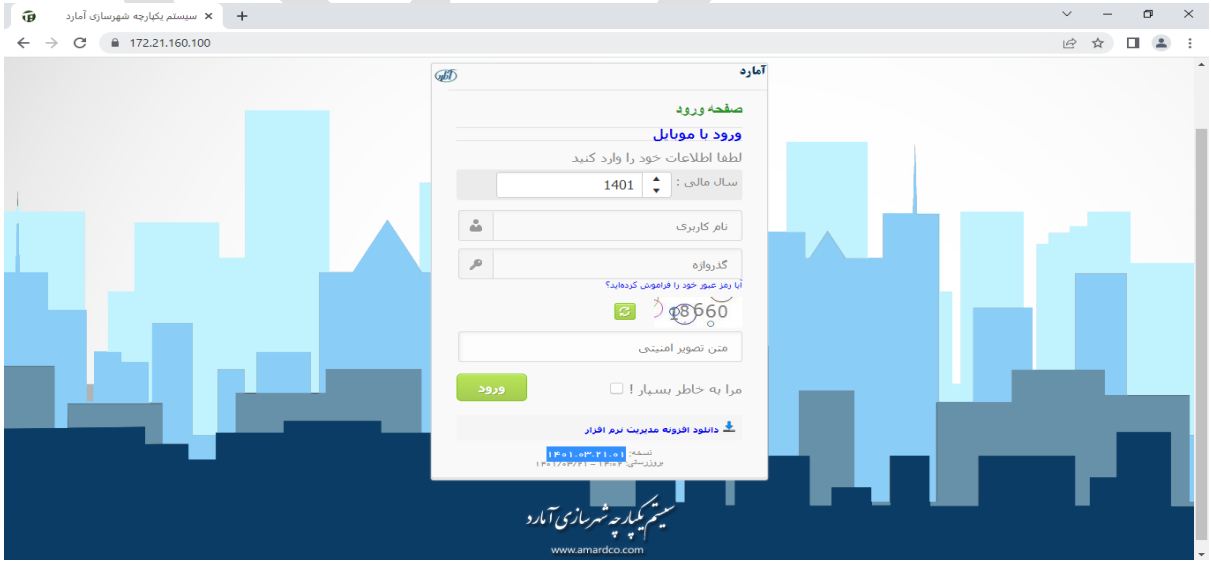
مشخصات محصول مورد آزمون			
نوع سیستم:	تحت وب	زبان برنامه نویسی	ASP.NET
نسخه‌ی محصول:	1401.03.21.01	تکنولوژی	.NET
مشخصات سرور:	Windows Server	نسخه‌ی سرور	2019
پایگاه داده:	MicrosoftSQLServer	نسخه پایگاه داده	2019
قابلیت‌های محصول	**منوی اصلی برنامه کاربردی تحت وب(سیستم یکپارچه شهرسازی آمارد) و قابلیت‌های آن در ادامه آورده شده است:** ▪ تعاریف ▪ درآمد ▪ پرونده ▪ نوسازی ▪ گزارشات ▪ ماده صد ▪ مدیریت کاربران ▪ جستجو و بازبینی ▪ امکانات ▪ آرشیو ▪ بایگانی ▪ ممیزی ▪ اصناف ▪ رویدادهای ممیزی		
جزئیات فایل‌های اجرایی برنامه کاربردی	به دلیل تعدد فایل‌های اجرایی سامانه، مقادیر درهم‌سازی شده فایل‌های اجرایی در این گزارش ارائه نشده است. این مقادیر در گزارش‌های بایگانی شده در آزمایشگاه ثبت شده و در صورت نیاز قابل ارائه است.		
ارتباطات			
• ارتباط با سرور پیام کوتاه			

۱-۲- پیکربندی هدف ارزیابی

در این بخش پیکربندی محصول شرح داده می‌شود، و در این بین آنهایی که در ارزیابی پوشش داده شده‌اند مشخص می‌گردند.



شکل ۱-۱: سناریو پیشنهادی تولیدکننده جهت قرارگیری محصول در محیط عملیاتی



شکل ۲-۱: صفحه‌ی ورود به سامانه

۲- عدم انطباق‌های محصول

در این بخش عدم‌انطباق‌های محصول در دو گروه الزامات کارکرد امنیتی، الزامات تضمین امنیت، ارایه شده‌است.

توجه:

- عدم انطباق‌ها در حوزه‌های الزامات ASVS و آسیب‌پذیری‌ها در گزارش فاز دوم آزمون منعکس خواهد شد.
- نظر به محدودیت‌های زمانی، در گزارش آزمون به نمونه‌هایی از مصادیق عدم انطباق با الزامات استانداردها و آسیب پذیری که در زمان آزمون شناسایی و بهره‌برداری شده‌اند، پرداخته می‌شود. در نتیجه جهت حصول اطمینان از رفع عدم انطباق‌ها، لازم است اقداماتی جهت بازبینی کامل محصول از منظر رفع ایرادات و در کلیه‌ی بخش‌ها صورت پذیرد.

۲-۱- الزامات کارکرد امنیتی

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
۱	ممیزی امنیت	FAU_GEN.1.1	توابع امنیتی هدف ارزیابی باید قادر به تولید رکوردهای ممیزی براساس رخدادهای قابل ممیزی زیر باشد: • ورود و خروج کاربر به/ از سیستم • رویدادهای قابل ممیزی ذکر شده در جدول مربوطه در پروفایل حفاظتی • دیگر موارد: اختصاص: دیگر رویدادهای قابل ممیزی	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			✓ رویدادهای ممیزی قابل ثبت در این سامانه شامل تمام رویدادهای مطرح شده در پروفایل حفاظتی نمی‌شود. نمونه هایی از رویدادهای غیر قابل ثبت در ادامه آورده شده است: - تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی(FAU_SAR.2): از تلاش‌های غیرمجاز جهت خواندن رکوردهای ممیزی، لاگ تهیه نمی‌شود. - عملیات انجام شده در صورت پیشی‌گرفتن از آستانه‌ی تعیین شده برای ذخیره‌ی رویدادهای ممیزی(FAU_STG.3): حدآستانه قابل تنظیم برای ذخیره رویدادهای ممیزی وجود ندارد، لازم است بعد از پیاده‌سازی این عملیات، رکوردی از آن در رویدادهای ممیزی ثبت گردد. - عملیات انجام شده به دلیل شکست ذخیره‌سازی ممیزی(FAU_STG.4): در صورتی‌که حافظه هارد دیسک سیستم سرور پایگاه داده و فضای اختصاص داده شده به جداول پایگاه داده به صورت کامل پر شود، اقدامی از سمت سامانه نرم افزاری صورت نمی گیرد و پیامکی مبنی بر اطلاع رسانی به مدیر سیستم ارسال نمی شود و رویداد ممیزی ثبت نمی گردد. - درخواست های موفق برای اجرای عملیات بر روی یک موجودیت غیرفعال تحت پوشش سیاست توابع امنیتی(FDP_ACF.1): از هر نوع عملیات دستیابی به	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			موجودیت‌ها در سامانه اعم از درخواست ناموفق، ویرایش اطلاعات کاربران ، ایجاد کاربران و غیره رکوردی در رویدادهای ممیزی ثبت نمی‌شود. - رسیدن به حد آستانه برای تلاش های احرازهویت ناموفق و اقداماتی که انجام می شود (FIA_AFL.1) : در سامانه نرم افزاری سیستم یکپارچه شهرسازی آمارد، در صورت رسیدن به حد آستانه «تعداد ورودهای ناموفق مجاز» کاربر قفل می شود، اما از آن ممیزی تهیه نمی‌شود. - استفاده ناموفق از مکانیزم احرازهویت (FIA_UAU.1): به ازای تلاش‌های ناموفق برای ورود، رکورد ممیزی ثبت نمی‌شود. تنها ورود موفق به سامانه ثبت می‌شود. به ازای تلاش های ناموفق کاربر غیرفعال شده جهت لاگین، لاگ ثبت نمیشود. - استفاده ناموفق از مکانیزم شناسایی کاربر، از جمله هویت کاربران ارائه شده (FIA_UID.1): باتوجه به آنکه شناسایی و احرازهویت در سامانه تحت وب به صورت همزمان انجام می گیرد، مشابه با FIA_UAU.1 در نظر گرفته می شود. - پیوند ناموفق ویژگی های امنیتی کاربر با موجودیت فعال (برای مثال ایجاد یک کاربر)(FIA_USB.1): در خصوص مؤلفه‌ی FIA_USB.1 منظور از ایجاد کاربر ایجاد کاربر فعال یا همان ایجاد نشست است. درصورتی که کاربر اقدام به ورود به سامانه کند، رکوردهای مبنی بر ورود موفق/ناموفق، و رکوردهای مربوط به برقراری/عدم برقراری	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			نشست (الزام FTA_TSE) ثبت شود کفایت می‌کند. به ازای ایجاد موفق کاربر لاگ ثبت می شود. اما از تلاش‌های ناموفق کاربر برای ورود، رکوردی در رویدادهای ممیزی ثبت نمی گردد. - تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی(FMT_MSA.1): عملکرد مدیر بر روی مشخصه‌های امنیتی قابل تغییر توسط مدیر مانند مجوزها و نقش‌های کاربر در رویدادهای ممیزی ثبت نمی‌شود. به عنوان مثال، با عضو نمودن یک کاربر در گروه، یا با حذف یک کاربر از گروه، هیچ رویداد ممیزی ثبت نمی گردد. همچنین با اعطای دسترسی یا سلب و حذف دسترسی از گروه، رکوردی از آن در دسته رویدادهای ممیزی ثبت نمی گردد. همچنین از تغییر مجوز دسترسی به صورت مستقیم به کاربران، از طریق منوی مدیریت کاربران/دسترسی به کارتابل، هیچ رکورد ممیزی ثبت نمی شود. - تمامی تغییرات بر روی مقادیر داده‌های امنیتی (FMT_MTD.1): این الزام در مورد داده توابع امنیتی مانند رکوردهای ممیزی و ویرایش اطلاعات پروفایل و رمز عبور کاربران می‌باشد. در این سامانه امکان اعمال تغییر به داده‌های توابع امنیتی هدف ارزیابی وجود دارد که از این تغییرات در اطلاعات پروفایل، رکوردی در رویدادهای ممیزی ثبت نمی‌شود. مثلا در این سامانه با تغییر رمز عبور یا ویرایش پروفایل کاربران، توسط ادمین، رویدادی ثبت نمی گردد. (لازم به ذکر است از تغییر تنظیمات تعداد تلاش	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			ناموفق احراز هویت و تغییر مدت زمان انقضای نشست، تغییر حداقل طول کلمه عبور، رویداد ممیزی تغییر تنظیمات ممیزی آنها، به صورت کلی و با عنوان کلی " تغییر تنظیمات" ثبت می گردد) در سامانه امکان حذف رکوردهای ممیزی از منوی رویدادهای ممیزی/لاگین های کاربران، برای مدیرسیستم فراهم شده است اگرچه رکورد لاگی از حذف رویدادهای ممیزی توسط مدیر، در سامانه ثبت نمی گردد. - استفاده از توابع مدیریتی(FMT_SMF.1) : باید از اقدامات مدیریتی انجام شده توسط مدیر سیستم، ممیزی تهیه شود که در این سامانه بصورت کامل برقرار نمی باشد. - تغییرات بر روی گروهی از کاربران بخشی از یک نقش (FMT_SMR.1):از طریق منوی مدیریت کاربران/ دسترسی و گروه بندی کاربران، با انتخاب منطقه یاسازمان شهرداری مرکزی، و با انتخاب هریک از نقش ها، و کلیک بر روی حذف واضافه کردن اعضا، می توان به آن گروه عضوی را اضافه نموده یا از گروه مدنظر، عضوی حذف گردد که براساس رویداد FMT_MSA.1، با عضو نمودن یک کاربر در گروه، یا با حذف یک کاربر از گروه، هیچ رویداد ممیزی ثبت نمی گردد. - هر شکستی که توسط توابع امنیتی شناسایی می‌شود، همه قابلیت های محصول که به علت شکست متوقف می‌شود(FRU_FLT.1): خطاهای برنامه در واسط کاربری سامانه از طریق منوی امکانات/ بررسی پیام های سیستم، ذخیره می گردد که آخرین شماره آن	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			۱۳۲۹۸ می باشد و آخرین تاریخ آن مربوط به Mon Feb 08 2021 10:06:49 هست و با زدن شماره ۱۳۲۹۹ دیگر خطایی در واسط کاربری سامانه نمایش داده نمی شود. همچنین بعضی از خطاها درIIS سرور در مسیر E:\Amard\Shahrsazi\publish\App_Data\ErrorsLog ذخیره می گردد که در واسط کاربری سامانه نمایش داده نمی شوند. بنابراین باتوجه به اینکه خطاهای مطرح شده، خطاهای مورد نظر الزام نبوده و لاگ ممیزی از خطاهای برنامه ثبت نمی گردد، لذا الزام مورد قبول نخواهد بود و رد می گردد. - عدم پذیرش یک نشست جدید بر اساس محدودیت چندین نشت های همزمان(FTA_MCS.1): در سامانه نرم افزاری سیستم یکپارچه شهرسازی آمارد، برای کاربران زمانیکه یک نشست جدید باید برقرار شود، اگر از حداکثر تعداد نشست همزمان یک کاربر بیشتر شود، اجازه ورود کاربر به سامانه را نمی دهد و کاربر با خطای حداکثر تعداد نشست (مقدار تنظیم شده در فیلد حداکثر تعداد نشست) می باشد مواجه می شود و از برقراری نشست جدید اجتناب می گردد. اما رکوردی از آن در رویدادهای ممیزی ثبت نمی گردد، بنابراین الزام رد می گردد. - پایان دادن به یک نشست توسط مکانیزم قفل نشست(FTA_SSL.3): ادعای سندST: محصول همچنین نشست هایی که بعد از ۲ ساعت هیچ فعالیتی نداشته اند را غیر فعال	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			می نماید. در واسط کاربری سامانه نرم افزاری سیستم یکپارچه شهرسازی آمارد، امکان تغییر زمان غیرفعال بودن کاربر برای مدیر سیستم از طریق منوی تعاریف←پنل کاربری←تنظیمات لاگین و با مقدار دادن به فیلد خاتمه نشست بعد از چند دقیقه وجود دارد. بعد از بررسی صورت گرفته سامانه، طی مدت زمان تنظیم شده برحسب دقیقه برای غیرفعال بودن، نشست کاربر خاتمه نمی یابد و همچنان به فعالیت خود در سامانه ادامه می دهد.[1] لازم است بعد از پیاده سازی رکوردی از آن در رویدادهای ممیزی ثبت گردد. - جلوگیری از ایجاد نشست بر اساس مکانیزم‌های ایجاد نشست(FTA_TSE.1) : در سامانه می‌توان در بخش « تعاریف/پنل کاربری/محدودسازی لاگین »، محدوده IP غیر مجاز برای ورود کاربر تعریف نمود. این بازه IP به تمامی کاربران اعمال می‌شود. درصورتی‌که کاربر در خارج از محدوده رنج تعیین شده آی پی که محدوده غیرمجاز IP می باشد اقدام به ورود کند، با پیام خطای شما با این آی پی قادر به لاگین نیستید، مواجه شده ولی رویداد ممیزی برای کاربر ثبت نمی گردد. علاوه بر این با محدود نمودن تاریخ، رویداد ممیزی از عدم ورود کاربر به سامانه در خارج از رنج محدوده	

[1] طبق ایمیل دریافتی از نماینده محترم شرکت آمارد، درخصوص غیر فعال نمودن تنظیمات نشست هایی که بعد از ۲ ساعت هیچ فعالیتی نداشته اند، اعلام نمودند که به سبب اینکه کارتابل هر چند ثانیه refresh و به روز رسانی می شود Session منقضی نمی‌شود.

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			تعیین شـــده، ثبت نمی شـــود. همچنین به ازای تلاش های ناموفق کاربر غیرفعال شـــده جهت لاگین، لاگ ثبت نمی‌شود.	
۲		FAU_SAR.1.2	توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی را به شکل مناسبی برای کاربر، جهت تفسیر اطلاعات فراهم نماید. ✓ به ازای بعضی eventها، رویداد ممیزی به صورت واضح و قابل فهم برای کاربر نمایش داده نمی شود. این موارد در ادامه لیست شده است: - در رویداد مربوط به FAU_SAR.1 به محض ورود کاربر به صفحه امکانات/ گزارش کاربران سیستم، کاربر می تواند قبل از جستجوی رویدادهای ممیزی، رویدادهای ممیزی مربوط به روز جاری را مشاهده نماید که رکورد لاگی از آن در منوی رویدادهای ممیزی/ لاگین های کاربران، با عنوان مشاهده کننده، ثبت می‌گردد، اما فقط تاریخ مشاهده لاگ کاربر، بدون ساعت، ثبت شده است و مشخص نیست که دقیقا کاربر در چه تایم و ساعتی رویدادهای ممیزی را مشاهده نموده است. همچنین اختلال در ثبت لاگ هم در الزام FAU_SAR.1 وجود دارد و در صورت مشاهده‌ی لاگ توسط یک کاربر لاگ مربوطه گاهاً با تأخیر ثبت شده و یا ثبت نمی‌شود. - در رویداد مربوط به FTA_SSL.4، وقتی کاربر دکمه خروج را می‌زند، در منوی رویدادهای ممیزی/ لاگین های کاربران، رکورد ممیزی با عنوان (ورود/خروج کننده)	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			ثبت می‌شود که اگر کاربر به سامانه لاگین نموده است، تاریخ ورود و اگر از سیستم خروج کرده است، تاریخ خروج نمایش داده می شود. اما ساعت ورود یا خروج کاربر در سیستم ثبت نمی‌شود و فقط تاریخ آن در سامانه قابل نمایش است. - در رویداد مربوط به FMT_MOF.1، با تغییر تنظیمات سیاست پیچیدگی پسورد یا فعال نمودن احراز هویت دومرحله ای و ... توسط admin رکوردی از لاگ ثبت می شود. اما فقط در رکورد رویداد ممیزی ثبت شده، نوع عملیات(نوع رویداد): ویرایش تنظیمات و در شرح عملیات: تغییر در تنظیمات، ثبت می شود و مشخص نیست که چه تنظیماتی توسط مدیر سیستم صورت گرفته است. - در رویداد مربوط به FMT_MTD.1(1)، با تغییر مقادیر پارامتر هر یک از فیلدهای تنظیمات، مشخص نیست که دقیقا مقادیر پارامتر کدام فیلد از چه مقداری به چه مقداری، توسط کاربر admin تغییر داده شده است و رویداد ممیزی ذخیره شده فقط با عنوان کلی "تغییر تنظیمات" ثبت می‌گردد. - در رویداد مربوط به FMT_SMR.1، با تغییر نقش کاربر، از منوی مدیریت کاربران/سطح دسترسی، رکورد ممیزی با عنوان کلی "تعریف سطح دسترسی" ثبت می‌گردد و دقیقا مشخص نیست که کدام مجوزهای سطح دسترسی به کاربر اختصاص داده شده و چه مجوزهایی از کاربر، سلب دسترسی شده است.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			- در رویداد مربوط به FIA_UAU.5، رویداد ممیزی از لاگین نمودن کاربر با احراز هویت دومرحله ای در رویدادهای ممیزی/ لاگین های کابران، ثبت می شود، اما لاگ ثبت شده تحت عنوان کلی ورود/خروج کننده ثبت می شود و مشخص نیست که کاربر با احراز هویت دومرحله ای لاگین نموده است و در درک لاگ ها ابهام دارد.	
۳		FAU_SAR.2.1	توابع امنیتی هدف ارزیابی باید از دسترسی کلیه کاربران جهت خواندن رکوردهای ممیزی ممانعت نماید، بجز کاربرانی که به آنها مجوز دسترسی با قابلیت خواندن داده شده باشد. با توجه به اینکه از دسترسی کاربر غیرمجاز به بخش ممیزی ممانعت به عمل نیامده است، بنابراین این بند قبول نمی گردد. باید طبق الزام بازبینی رویدادهای ممیزی فقط مختص مدیر سیستم و کاربرانی که دارای دسترسی هستند، باشد. اما Logهای elmah بدون احراز هویت و از طریق لینک زیر در دسترس هستند. https://172.21.160.100/elmah بنابراین، کاربر غیرمجاز، می تواند بدون احراز هویت، نیز به رویدادهای ممیزی، دسترسی داشته باشد و از دسترسی کلیه کاربران جهت خواندن رکوردهای ممیزی ممانعتی به عمل نیامده است. با توجه به موارد مطرح شده، بنابراین الزام قبول نمی گردد.	
۴		FAU_SAR.3.1	توابع امنیتی هدف ارزیابی باید امکان اعمال روش انتخاب و مرتب سازی را فراهم نماید تاداده ممیزی براساس حساب کاربری، روش اتصال، تاریخ/زمان، موقعیت، رکوردها و مستندات مورد	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			بحث رخدادها (در صورت امکان)، نوع رخداد، گروه کاربر (در صورت امکان)، و/یا سطح حساسیت رکوردهای ممیزی، مرتب/انتخاب شوند. ✓ با توجه به عدم امکان فیلتر رکوردهای ممیزی ذخیره شده براساس نام کاربری و براساس آی پی یا موقعیت، الزام رد می‌گردد. - در واسط کاربری سامانه از منوی امکانات/گزارش کاربران سیستم، امکان مرتب‌سازی رکوردهای ممیزی فقط براساس فیلد تاریخ وجود دارد. باید طبق الزام امکان مرتب سازی بر اساس نوع رویداد، شناسه کاربری نیز اعمال گردد. - همچنین در سامانه نرم افزاری سیستم یکپارچه شهرسازی آمارد، باید امکان فیلتر و مرتب سازی رکوردهای ممیزی ذخیره شده براساس نام کاربری، آی پی یا موقعیت، نوع رویداد، تاریخ و زمان رویداد بر روی رویدادهای ممیزی از منوی رویدادهای ممیزی/لاگین های کاربران، نیز اعمال گردد.	
۵		FAU_SEL.1.1	محصول باید قادر باشد براساس مشخصه‌های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادها را جهت ممیزی شدن، انتخاب نماید: • هویت موجودیت فعال، نوع رخداد • تنها رخدادهای ممیزی کم‌اهمیت باید برای عدم ثبت در فایل‌های ممیزی انتخاب شوند.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			✓ شـواهدی مبنی بر رویدادهای ممیزی انتخابی که به واسـطه آن بتوان رویدادهای قابل ثبت را تغییر داد در سیستم وجود ندارد و الزام مورد قبول نیست.	
۶		FAU_STG.1.1	توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی ذخیره شده در دنباله ممیزی را از حذف غیر مجاز حفاظت نماید. ✓ در این سامانه دکمه "حذف همه" در منوی رویدادهای ممیزی/لاگین های کاربران، برای کاربرانی که مجوز مربوطه به آنها اعطا شده است در دسترس می‌باشد. اگرچه با استفاده از پروکسی وintercept نمودن درخواست حذف همه رویدادها و جایگزینی شناسه‌ی نشست کاربر سطح پایین در درخواست مربوطه، اجرای غیر مجاز درخواست محرز شده است. بنابراین با توجه به حذف لاگ از طریق دکمه "حذف همه"، در واسط کاربری سامانه لذا الزام مورد تایید نخواهد و رد می گردد.	
۷		FAU_STG.1.2	توابع امنیتی هدف ارزیابی باید قادر به جلوگیری از تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده در دنباله ممیزی باشد. ✓ ادعای سندST: محصول قادر به تشخیص تغییرات غیر مجاز در رکوردهای ممیزی است. - در جداول حاوی رکوردهای لاگ در دیتابیس، فیلدی مشاهده نشد که حاوی موارد هش یا رمز شده آن رکوردها باشد. بنابراین ظاهرا مکانیسمی برای کنترل صحت پیاده سازی نشده است و رد می گردد. در صورت تغییر در رکوردهای جدول	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			[AmardShahrsazi].[dbo].[History] در پایگاه داده سامانه، رکورد ذخیره شده و داده نمایش داده شده در سامانه تغییر می‌یابد، بدون آن‌که این تغییر قابل تشخیص باشد. جداول حاوی رکوردهای لاگ در دیتابیس شامل جدول های [AmardShahrsazi].[dbo].[accesslevel]، [AmardShahrsazi].[dbo].[History]، [AmardShahrsazi].[dbo].[LoginHistory]، [AmardShahrsazi].[dbo].[LogException]، [AmardShahrsazi].[dbo].[UserLogined] می باشند.	
۸		FAU_STG.3.1	توابع امنیتی هدف ارزیابی در صورت تجاوز دنباله ممیزی از محدودیت از پیش تعریف شده باید با استفاده از یک کانال ارتباطی، پیام کوتاه یا معادل آن، کاربران مربوطه را مطلع نماید. ✓ ادعای سند ST : محصول در صورت تجاوز دنباله ممیزی از فضای آزاد هارد سیستم کاربر مربوطه را مطلع کرده و در این حالت رویدادهای ممیزی را نادیده می گیرد.[۱] - حدآستانه قابل تنظیمی برای ذخیره رویدادهای ممیزی در واسط کاربری سامانه وجود ندارد و تنظیمات و پیکربندی مربوطه انجام نشده است. همچنین در حین ارزیابی الزام بعدی و پرشدن حجم جدول [AmardShahrsazi].[dbo].[UserLogined]پیامکی مبنی بر عبور از آستانه ارسال نشد.	

[۱] اگرچه طبق ایمیل دریافتی از نماینده محترم شرکت آمارد، برای آستانه لاگ ها(حدآستانه رویدادنگاری) کاری انجام نشده است و برای رویدادهای ممیزی حدآستانه ای در نظر گرفته نشده است.

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
۹		FAU_STG.4.1	توابع امنیتی هدف ارزیابی در صورت پر شدن دنباله ممیزی، باید علاوه بر ارسال هشدار، یکی از اقدامات زیر را انجام دهد: • رویدادهای ممیزی را نادیده بگیرد. • از ذخیره رویدادهای قابل ممیزی، بجز آنهایی که توسط کاربر مجاز و تحت حقوق خاص رخ می دهند، جلوگیری نماید. • بر روی قدیمی ترین رکوردهای ممیزی ذخیره شده دوباره نویسی نماید. ✓ ادعای سندST : محصول در صورت تجاوز دنباله ممیزی از فضای آزاد هارد سیستم کاربر مربوطه را مطلع می کند. و در این حالت رویدادهای ممیزی را نادیده می گیرد. FAU_STG.3.1, FAU_STG.4.1 باتوجه به ادعای سند ST، فضای هارد را پر نمودیم که با پر شدن کامل حجم اختصاص داده شده مشاهده می‌شود که فضای خالی پایگاه داده هنوز کامل پر نشده است. بنابراین حجم آزاد سیستم سرور پایگاه داده را با کد پر نمودیم و در Microsoft sql server management studio، با حلقه، اقدام به اضافه کردن رکورد به جدول [AmardShahrsazi].[dbo].[UserLogined] نمودیم. در نهایت با پر شدن کامل حجم اختصاص داده شده مشاهده می‌شود که کارکرد صحیح برنامه با مشکل مواجه می شود و سامانه قادر به نمایش رویدادهای ممیزی نیست. بنابراین به نظر می رسد که در هنگام پر شدن رویدادهای ممیزی، اقدامی از سمت سامانه نرم افزاری صورت نمی گیرد، لذا الزام مورد پذیرش نخواهد بود و رد می گردد.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
۱۰	پشتیبانی از رمزنگاری	FCS_COP.1.1(1)	توابع امنیتی هدف ارزیابی باید برای وارسی صحت داده‌های ممیزی و داده‌های رکورد بر اساس یک الگوریتم رمزنگاری مشخص و اندازه کلید رمزنگاری اجرا شود که مطابق با لیستی از استانداردها باشد. ✓ در محصول جهت وارسی صحت داده‌های ممیزی و داده‌های رکود از مکانیزم‌های مبتنی بر رمزنگاری استفاده نمی‌شود. دستکاری داده‌های رکورد و ممیزی در محصول قابل تشخیص نیست.	
۱۱		FCS_COP.1.1(2)	توابع امنیتی هدف ارزیابی باید تولید داده درهم‌سازی را بر اساس یک الگوریتم رمزنگاری مشخص و اندازه‌کلید رمزنگاری اجرا کند که مطابق با لیستی از استانداردها باشد. ✓ رمزعبور کاربران به صورت غیر شفاف ذخیره می شود، طبق شواهد در محصول از الگوریتم SHA1 استفاده شده است و برخلاف ادعای تولیدکننده در سند هدف امنیتی از الگوریتم SHA256 استفاده نشده است، خروجی ابزارهای آزمایشگاه با خروجی پایگاه داده یکسان نیست، با توجه به فراهم نشدن نیازمندی‌های آزمایشگاه امکان ارزیابی دقیق این الزام وجود ندارد.	
۱۲		FCS_TLSS_EXT.1.1	محصول باید TLSv1.2 و یا TLSv1.1 را با پشتیبانی از مجموعه‌های رمزهای مجاز مندرج در پروفایل حفاظتی پیاده‌سازی نماید.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			- ارتباط بین سامانه و کاربران، تحت پروتکلTLSv1.0 و TLSv1.1 و TLSv1.2 برقرار می‌شود، لازم است پروتکل‌های TLSv1.0 و TLSv1.1 بر روی سرور غیر فعال شوند. علاوه بر این در بین مجموعه رمزهایی که سرور از آن‌ها پشتیبانی می‌کند، مجموعه‌رمزهایی وجود دارند که طبق استاندارد غیرمجاز هستند. مجموعه رمزهای غیرمجاز در TLSv1.2 شامل موارد زیر است: TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) – C	
۱۳		FCS_TLSS_EXT.1.2	محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و یا TLS1.1، دارند، رد نماید. ✓ با sslscan، ارتباط را باTLSv1.1، TLSv1.0 برقرار کرده و مشاهده می‌شود که سامانه ارتباط را برقرار می‌کند. بنابراین الزام مورد تایید نخواهد بود و رد می گردد.	
۱۴		FCS_TLSS_EXT.1.3	محصول باید پارامترهای ساخت کلید را با استفاده از • RSA با اندازه کلید ۲۰۴۸ بیت و یا ۳۰۷۲ بیت و ۴۰۹۶ بیت و یا • منحنی‌های NIST secp256r1 و یاsecp384r1 و یا • پارامترهای DiffeHellman با اندازه‌ی ۲۰۴۸ و یا ۳۰۷۲ بیت ایجاد نماید. ✓ طبق بررسی به عمل آمده، محصول از elliptic curve غیرمجاز زیر پشتیبانی می‌کند. Curve 25519 DHE 253	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
۱۵	شناسایی و احراز هویت	FIA_AFL.1.2	زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید یا از آن بیشتر شد، توابع امنیتی هدف ارزیابی باید اقداماتی را که بدین منظور در نظر گرفته شده است، انجام دهند. یکی از این اقدامات می تواند پیچیده تر کردن عمل احراز هویت مجدد کاربر باشد. ✓ علی‌الرغم وجود تنظیمات مدت زمان مسدودی (فعالسازی حساب بعد از چند ثانیه)، تنظیمات به درستی عمل نکرده و کاربر پس از گذشت زمان مذکور قادر به ورود به سامانه نخواهد بود. لازم به ذکر است ادمین سامانه می تواند کاربر را از طریق منوی مدیریت کاربران←تعریف کاربران، مجددا فعال نماید.	
۱۶		FIA_ATD.1.1	توابع امنیتی هدف ارزیابی، باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید: ۱- شناسه کاربر یا کلمه عبور/پین برای کارت شناسایی هوشمند ۲- متد احرازهویت مورد استفاده ۳- داده های احراز هویت ۴- نقش کاربر ۵- وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره) و ۶- یا هر مشخصه امنیتی دیگر	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			✓ در این سامانه، داده های احراز هویت برای کاربر admin به درستی نگه داشته نمی شود و کاربر admin با هر کلمه عبوری(پسورد) می تواند به سامانه لاگین و ورود نماید. بنابراین الزام مورد تایید نخواهد بود و رد می گردد.	
۱۷		FIA_UAU.1.2	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. ✓ برای URL های مربوط به بخش ادمین و سایر کاربران، مکانیزم احراز هویت رعایت نشده است. با توجه به اینکه کاربر احراز هویت نشده می‌تولند به توابع و صفحات داخلی دسترسی داشته باشد، الزام قبول نمی شود. در صورت ارسال درخواست به صفحات داخلی توسط کاربر احراز هویت نشده به صفحه مورد نظر دسترسی پیدا می کند.	
۱۸		FIA_UAU.5.2	توابع امنیتی هدف ارزیابی هویت هر کاربر را مطابق با کاربران از راه دور باید از دومین روش احرازهویت که در الزام FIA_UAU.5.1 تعریف شده استفاده نمایند، به عبارت دیگر علاوه بر بررسی نام کاربری و احرازهویت از متد احرازهویت ثانویه نیز استفاده نماید، قوانینی که چگونگی احرازهویت نمودن توسط چندین مکانیسم احرازهویت را وصف می‌نمایند. ✓ با توجه به اینکه در سامانه آمارد، می‌توان بدون وارد کردن کد احراز هویت مرحله دوم به سیستم دسترسی داشت. درواقع به واسطه‌ی تنظیم شناسه‌ی نشست در پاسخ درخواست مرحله‌ی اول احراز هویت، با false نمودن isEnabledTwoFactorLogin در پاسخ دریافتی از	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			سـرور می‌توان مرحله‌ی دوم احراز هویت را دور زد. بنابراین الزام مورد تایید نخواهد بود و رد می گردد.	
۱۹		FIA_UID.1.2	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. ✓ عطف به الزام FIA_UAU.1.2، این الزام مورد قبول نیست.	
۲۰		FIA_USB.1.1	توابع امنیتی هدف ارزیابی باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید: - شناسه کاربر - نقش‌های کاربر - جزئیات واسط کلاینت - پیشینه احرازهویت (زمان آخرین تلاش احرازهویت موفق و ناموفق) - پیشینه دسترسی به سند/رکورد اخیر - لیست دیگر مشخصه‌های کاربری ✓ شناسه‌ی کاربر: تغییر در شناسه‌ی کاربر توسط مدیر سیستم در حین نشست فعال آن کاربر منجر به خاتمه‌ی نشست نشده و کاربر قادر به ادامه‌ی فعالیت خواهد بود.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			• جزئیات واسط کلاینت: سامانه State جزئیات واسط کلاینت که نشست از طریق آن ایجاد شده است را نگهداری نمی کند. با تغییر واسط کلاینت، نشست کاربر همچنان برقرار است و خاتمه نمی یابد. - پیشینه دسترسی به سند/رکورد اخیر: با توجه به عدم عملکرد صحیح توابع idle timeout، شواهدی مبنی بر نگهداری پیشینه دسترسی به سند/رکورد اخیر مشاهده نشد.	
۲۱		FIA_USB.1.3	توابع امنیتی هدف ارزیابی باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید: هیچ تغییری در طول نشست فعال مجاز نمی‌باشد. - شناسه‌ی کاربر: تغییر در شناسه‌ی کاربر توسط مدیر سیستم در حین نشست فعال آن کاربر منجر به خاتمه‌ی نشست نشده و کاربر قادر به ادامه‌ی فعالیت خواهد بود. - در صورتی که کاربر غیرفعال شود از سیستم خارج نمی شود و همچنان به منوهای سامانه دسترسی دارد و فقط از ورود بعدی او ممانعت بعمل می‌آید و کاربر می تواند به فعالیت خود در سامانه ادامه دهد، لذا الزام مورد تایید نخواهد بود. - با تغییر واسط کلاینت، نشست کاربر همچنان برقرار است و خاتمه نمی یابد.	
۲۲		FIA_PMG_EXT.1.1	توابع امنیتی هدف ارزیابی باید قابلیت‌های مدیریت رمزعبور را که در زیرذکر شده‌اند برای رمزهای عبور سرپرستی فراهم نماید:	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			۱. رمزهای عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و حداقل یکی از کاراکترهای خاص ("@"، "#"، "$"، "٪"، "^"، "!" "&"، "×"، "(" , ")" و... باشند. ۲. حداقل طول رمزعبور باید توسط سرپرست امنیت، قابل تنظیم بوده و۱۵کاراکتر یا بیشتر باشد. در این سامانه اگرچه تنظیمات پیچیدگی پسورد و حداقل طول در هنگام ریست کردن پسورد توسط مدیر اعمال می‌شود، اما در تغییر رمز عبور توسط خود کاربر، سیاست‌های مذکور اعمال نمی‌شود و امکان تعریف پسورد ساده توسط کاربران فراهم است. لازم به ذکر است سیاستی که برای پیچیدگی پسورد در نظر گرفته می‌شود باید حتما در سمت سرور اعمال گردد.	
۲۳	حفاظت از داده‌های کاربری	FDP_ACF.1.1	توابع امنیتی هدف ارزیابی باید خط‌مشی‌های کنترل دسترسی را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید: • هویت کاربر • نقش‌ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند ✓ در سامانه سیستم یکپارچه شهرسازی آمارد، درخواست یک کاربر سطح بالا با پروکسی دریافت شد. سپس مقادیر کوکی .ASP.NET_SessionId و کوکیASPXAUTH. و پارامتر	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			AmardShahrsaziUserName مربوط به کاربر سطح پایین که دسترسی به ویرایش مشخصات مامور بازدید ندارد، را در درخواست کاربر سطح بالا جایگزین نمودیم. نتیجه آن شد که کاربری با سطح دسترسی پایین (نقش کاربر عادی) که اجازه دسترسی به عملکردها و توابع کاربر سطح بالارا ندارد، با استفاده از پروکسی می‌تواند به ویرایش مشخصات مامور بازدید، دسترسی داشته باشد و مقادیر آنها را تغییر دهد. بنابراین با توجه به ایراد مشاهده شده در مکانیزم access control می توان به دسترسی های کاربر سطح بالا دسترسی پیدا نمودو الزام مورد قبول نیست. لازم به ذکر است درخواست فوق به عنوان نمونه مطرح شده و دسترسی غیر مجاز محدود به نمونه‌ی ارایه شده نیست.	
۲۴		FDP_ACF.1.2	توابع امنیتی هدف ارزیابی باید قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال کنترل شده و موجودیت غیرفعال کنترل شده را مجاز نمایند: عملیات تنها به شرطی مجاز است که لیست کنترل دسترسی دارای رکوردی است که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال دهد.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			✓ عطف به ایراد شرح داده شده در الزام FDP_ACF.1.1 در صورت عدم وجود دسترسی به ویرایش مشخصات مامور بازدید، کاربر سطح پایین نیز قادر به انجام عملیات خواهد بود. بنابراین الزام مورد تایید نخواهد بود و رد می گردد.	
۲۵		FDP_ACF.1.3	توابع امنیتی هدف ارزیابی باید براساس قوانین بیشتر که در ادامه آمده، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: • کاربران با مجوز سرپرست سیستم دارای دسترسی به هر رکورد و روش ارائه شده توسط توابع امنیتی هدف ارزیابی می‌باشند. • کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت دارای دسترسی به هر اطلاعات در دسترس عموم می‌باشند. • و یا دیگر قوانین ✓ در این سامانه منوی پنل کاربری فقط برای کاربرadmin قابل مشاهده است. اگرچه با استفاده از پروکسی، درخواست ارسالی به سرور جهت دستیابی به این منو دریافت شد. مشاهده می‌شود دسترسی به صفحه‌ی مذکور با شناسه‌ی نشست کاربر سطح پایین که در ظاهر به این بخش دسترسی ندارد امکان‌پذیر است. لذا الزام مورد تایید نخواهد بود و رد می گردد.	
۲۶		FDP_ITC.2.1	توابع امنیتی هدف ارزیابی باید در زمان ورود داده کاربری تحت کنترل خط‌مشی امنیتی، از خارج هدف ارزیابی خط‌مشی کنترل دسترسی را اعمال نماید.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			✓ کاربر با دسترسی به آپلود فایل در سامانه می‌تواند از طریق منوی تعاریف/ تعاریف، عکس برای آرم آپلود نماید و این صفحه و عملکردهای آن از دسترسی غیرمجاز کاربران بدون دسترسی به آن، محافظت می‌شود. کاربری با سطح دسترسی پایین (نقش کاربر عادی) که اجازه دسترسی به فایل‌های آپلود کاربر سطح بالا را ندارد، با درخواست آپلود فایل عکس، با استفاده از پروکسی burp suite می‌تواند به آن دسترسی داشته باشد. بنابراین با توجه به عدم رعایت مکانیزم access control الزام مورد تایید نخواهد بود و رد می گردد.	
۲۷		FDP_ETC.2.1	توابع امنیتی هدف ارزیابی باید در هنگام خروج داده کاربری تحت کنترل خط‌مشی امنیتی به خارج از هدف ارزیابی خط‌مشی کنترل دسترسی را اعمال نماید. ✓ کاربر با دسترسی به دانلود فایل در سامانه می‌تواند از طریق منوی آرشیو/ آرشیو الکترونیک، عکس دانلود نماید و این صفحه و عملکردهای آن از دسترسی غیرمجاز کاربران بدون دسترسی به آن، محافظت می‌شود. کاربری با سطح دسترسی پایین (نقش کاربر عادی) که اجازه دسترسی به فایل‌های دانلود کاربر سطح بالا را ندارد، با درخواست دانلود فایل عکس، با استفاده از پروکسی burp suite می‌تواند به آن دسترسی داشته باشد. بنابراین با توجه به عدم رعایت مکانیزم access control الزام مورد تایید نخواهد بود و رد می گردد.	
۲۸		FDP_SDI.2.1	توابع امنیتی هدف ارزیابی باید داده کاربری ذخیره شده در کانتینر تحت کنترل خود را با توجه به مشخصه‌های درهمسازی داده کاربری ذخیره شده برای خطای صحت، داده رکورد و داده ممیزی مانیتور نماید.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			✓ طبق بررسی‌های انجام شده برای کنترل صحت رکوردهای جداول حاوی داده کاربری شامل: جدول[accesslevel] (کاربران)، جدول نگاشت نقش‌ها شامل جداول [Dastresi]، [DastresiKartabl]، [User_Of_Groh]،[m_access] و جدول[History] (رویدادهای ممیزی) از امضای دیجیتال یا hash استفاده نمی‌شود. با توجه به این‌که الزام FDP_SDI.2.1 در مورد پیاده‌سازی مکانیزم کنترل صحت بر روی مجموعه‌ای از داده‌های کاربری حائز اهمیت در سیستم و اطلاعات کاربران، نقش‌ها و تنظیمات امنیتی در سیستم و داده‌های ممیزی است؛ لازم است که ردیف‌های این جداول با مقدار درهم‌سازی، تحت محافظت صحت داده قرار داده شوند.	
۲۹		FDP_SDI.2.2	هنگام تشخیص خطای صحت داده، توابع امنیتی هدف ارزیابی باید اقدام لازم را صورت دهد. ✓ با توجه به موارد مطرح شده در الزام FDP_SDI.2.1 ، در سامانه آمارد از هیچ مکانیسمی برای کنترل صحت رکوردها استفاده نمی شود. بنابراین خطای صحت داده ای در سیستم رخ نمی دهد که اقداماتی برای مقابله با آن انجام گردد.	
۳۰	مدیریت امنیت	FMT_SMF.1.1	توابع امنیتی هدف ارزیابی باید قادر به انجام کارکردهای مدیریتی زیر باشد: • کارکردهای مدیریتی آورده شده در جدول پروفایل حفاظتی • دیگر کارکردهای مدیریتی	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			✓ برخی از کارکردهای مدیریتی مطرح شده در جدول این الزام، در این محصول پیاده‌سازی نشده است: - پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی (FAU_SEL.1) : امکان انتخاب مجموعه‌ای از رویدادها جهت ممیزی شدن وجود ندارد. - پشتیبانی از حدآستانه (FAU_STG.3): حدآستانه مشخصی برای ذخیره رویدادهای ممیزی ثبت نشده است. محصول در صورت تجاوز دنباله ممیزی از یک محدودیت از پیش تعریف شده باید از طریق واسط‌های محصول مدیر سامانه را مطلع نماید، که این قابلیت وجود ندارد. - عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد. (FDP_SDI.2): با عطف به الزام FDP_SDI.2.1، مکانیزم تشخیص صحت بر روی جداول امنیتی و داده های حائز اهمیت از منطق برنامه پیاده سازی نشده است و در نتیجه در حال حاضر اقدامات مربوطه در صورت تشخیص خطای صحت مصداقی ندارد. - مدیریت احراز هویت ناموفق ۱(FIA_AFL.1): تنظیمات مدت زمان مسدودی توسط مدیر با تنظیم نمودن مقدار فعال سازی حساب بعد از چند ثانیه انجام می شود، اما به درستی پیکربندی نشده است و کار نمی‌کند.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			- تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد (FTA_SSL.3): در واسط کاربری سامانه نرم افزاری سیستم یکپارچه شهرسازی آمارد، امکان تغییر زمان غیرفعال بودن کاربر برای مدیر سیستم از طریق منوی تعاریف←پنل کاربری←تنظیمات لاگین و با مقدار دادن به فیلد خاتمه نشست بعد از چند دقیقه وجود دارد. بعد از بررسی صورت گرفته سامانه، طی مدت زمان تنظیم شده برحسب دقیقه برای غیرفعال بودن، نشست کاربر خاتمه نمی یابد و همچنان به فعالیت خود در سامانه ادامه می دهد. بنابراین با توجه به عدم عملکرد صحیح و مناسب امکان وجود تغییر زمان غیرفعال بودن کاربر توسط مدیر سیستم، الزام مورد تایید نخواهد بود.	
۳۱	حفاظت از توابع امنیتی هدف ارزیابی	FPT_TDC.1.2	توابع امنیتی هدف ارزیابی باید در زمان تفسیر داده‌های توابع امنیتی هدف ارزیابی از دیگر محصولات IT امن، از لیستی از قوانین تفسیر که توسط توابع امنیتی هدف ارزیابی به کار می‌روند استفاده نماید. ✓ در هر دو حالت عدم برقراری ارتباط و با وارد نمودن پسورد اشتباه، سامانه خطای یکسانی(ارسال پیامک با خطا مواجه شد) را نمایش می دهد و چون در واسط کاربری سامانه هیچ لاگ ممیزی از پیام ها ثبت نمی شود و در نمایش خطای پیام ها در واسط کاربری سامانه تمایزی قائل نمی شود، بنابراین نمی توان دلیل نمایش خطا را متوجه شد. با توجه به موارد مطرح شده الزام مورد تایید نخواهد بود و رد می گردد.	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
۳۲	دسترسی به هدف ارزیابی	FTA_SSL.3.1	توابع امنیتی هدف ارزیابی باید کلیه نشست‌های تعاملی راه دور[1]را پس از مدت زمان مشخص، زمان قابل تنظیم توسط سرپرست غیرفعال بودن، خاتمه دهد. ✓ در واسط کاربری سامانه نرم افزاری سیستم یکپارچه شهرسازی آمارد، امکان تغییر زمان غیرفعال بودن کاربر برای مدیر سیستم از طریق منوی تعاریف←پنل کاربری←تنظیمات لاگین و با مقدار دادن به فیلد خاتمه نشست بعد از چند دقیقه وجود دارد. بعد از بررسی صورت گرفته سامانه، طی مدت زمان تنظیم شده برحسب دقیقه برای غیرفعال بودن، نشست کاربر خاتمه نمی یابد و همچنان به فعالیت خود در سامانه ادامه می دهد.	
۳۳		FTA_TAH.1.1	در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید تاریخ، زمان، متد، مکان سه نشست آخر موفق برقرار شده را به کاربر نشان دهد. ✓ در صورت ورود موفق به سامانه هیچ اطلاعاتی از تاریخچه نشست‌های موفق برقرار شده به کاربر نمایش داده نمی‌شود. فقط کاربر Admin از طریق منوی تعاریف← پنل کاربری←سشن های کاربر و منوی تعاریف← پنل کاربری←لاگین های ناموفق، می تواند نشست های آنلاین و ورودهای ناموفق خود را مشاهده نماید. توجه: دسترسی به منوی پنل کاربری، فقط برای کاربر Admin سامانه، میسر می باشد و هیچ کاربر دیگری به پنل کاربری دسترسی ندارد.	

[1]Remote

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
۳۴		FTA_TAH.1.2	در صورت برقراری نشست موفق، توابع امنیتی هدف ارزیابی باید تاریخ، زمان، متد، مکان آخرین تلاش ناموفق برای برقراری نشست و تعداد تلاش های ناموفق از زمان آخرین نشست موفق برقرار شده را نمایش دهد. ✓ در این سامانه، هیچ اطلاعاتی از تاریخچه دسترسی برای نمایش به کاربر وجود ندارد. مدیر سیستم یا افرادی که دسترسی دارند از طریق منوی رویدادهای ممیزی←لاگین های کاربران می توانند اطلاعات ورود و خروج خود و سایر کاربران را مشاهده نمایند.	
۳۵		FTA_TAH.1.3	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. ✓ در این سامانه، هیچ اطلاعاتی از تاریخچه دسترسی برای نمایش به کاربر وجود ندارد.	
۳۶	کانال‌ها و مسیرهای مورد اعتماد	FTP_ITC.1.1 (SMS)	محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل SSH, TLS, HTTPS میان خود و موجودیت IT معتبر همچون سرور ممیزی، سرور احرازهویت، دیگر قابلیت‌ها 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. ✓ آدرس url مربوط به سرور پیامکی ، www.afe.ir/WebService/V7/BoxService.asmx است که در وب کانفیگ IIS سرور سامانه آمارد می باشد. سامانه پیامکی را بررسی نموده و مشاهده شد که سامانه پیامکی www.afe.ir با https در دسترس هست. اما با توجه به اینکه	نظر به عدم پشتیبانی از HTTPS و TLS، در ارتباط با سرور ارسال پیامک، الزامات مؤلفه‌های FCS_TLSC_EXT.1، FCS_TLSC_EXT.4، FIA_X509_EXT.1 و

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			سامانه آمارد، قادر به ارسال پیامک با https نمی باشد، لذا الزام مورد تایید نخواهد بود و رد می گردد.	FIA_X509_EXT.2 (مجموعاً ۸ الزام) در بخش محدودیت‌های ارزیابی منعکس شده‌اند. در صورت پیاده‌سازی ارتباط از طریق کانال امن در آزمون آتی مورد ارزیابی قرار خواهند گرفت.
۳۷		FTP_ITC.1.3 (SMS)	محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای لیست خدماتی که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند راه‌اندازی نماید. ✓ عطف به توضیح ارائه شده در شرح عدم انطباق الزام FTP_ITC.1.1 (SMS)، این الزام نیز مردود اعلام می‌گردد.	
۳۸		FTP_TRP.1.1	محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل IPsec, SSH, TLS, HTTPS برای ایجاد کانال ارتباطی امن بین خود و مدیر سیستم راه دور را داشته که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. ✓ سامانه نرم افزاری سیستم یکپارچه شهرسازی آمارد، در تحویل نهایی بر روی http به آزمایشگاه تحویل داده شده است و آدرس URL آن به صورت زیر است: http://172.21.160.100:5100/ توسط آزمایشگاه برای سامانه Certificate ساخته شد و توسط وب سرور سامانه که IIS است، فایل گواهی را به سامانه بایند نموده و از طریق https ، سامانه در دسترس قرار گرفت و آدرس URL آن به صورت زیر است:	

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق	ملاحظات
			https://172.21.160.100:443 ارتباط بین کلاینت و سرور تحت پروتکل های TLSv1.2 , TLSv1.1, TLSv1.0 انجام می شود. با توجه به اینکه در بین مجموعه رمزهایی که محصول از آن ها پشتیبانی می کند، مجموعه رمزهایی وجود دارند که طبق استاندارد غیر مجاز هستند، بنابراین الزام قبول نمی شود. مجموعه رمزهایی که در TLSv1.2 غیر مجاز هستند در زیر آورده شده است: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) – C همچنین مجموعه رمزهایی که در TLSv1.1, TLSv1.0 غیر مجاز هستند در زیر آورده شده است: TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 4096) – C	

۲-۲- الزامات تضمین امنیت

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق
۱	تولید و توسعه(ADV)	ADV_FSP.1.1E	ارزیاب باید تایید کند که اطلاعات فراهم شده نیازمندی‌های مربوط به مفاهیم و ارایه شواهد مرتبط را برآورده می‌کند. - معرفی واسط‌ها جامع و کامل نیست. همچنین با توجه به نگاشت‌های انجام شده، برای تمامی کارکردها، تمامی پارامترهای ورودی و خروجی آن کارکرد در جدول مربوطه ذکر نشده‌است.
۲		ADV_FSP.1.2E	ارزیاب باید مشخص نماید که خصوصیات عملکردی موجود به صورت دقیق و جامع تمامی‌نیازمندها را برآورده می‌کند. - پس از بررسی نگاشت انجام شده، و بررسی الزام‌های کارکردی امنیت و همچنین واسط‌ها مشخص شد نگاشت انجام شده توسط تولیدکننده، کامل نیست و نگاشت با بعضی از الزامات انجام نشده است. - الزاماتی وجود دارد که به واسط‌های معرفی شده در این سند اشتباهاً map شده‌اند، نتیجه می‌گیریم نگاشت انجام شده دقیق نیست. در ازای هر واسط نگاشت به کلیه الزامات کلاس واسط داده شده است در حالی که براساس هدف تعریف شده در واسط این چنین نیست.
۳	اسناد راهنما(AGD)	AGD_OPE.1.1E	ارزیاب باید تایید کند که اطلاعات فراهم شـــده نیازمندی‌های مربوط به مفاهیم و ارایه شـــواهد مرتبط را برآورده می‌کند. - بخش نقش‌ها ایراداتی دارد و کامل نیست.

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق
			- بخش واسط‌ها ایراداتی دارد و کامل نیست.
۴	ارزیابی هدف امنیتی(ASE)	ASE_INT.1.1E	ارزیاب باید تایید کند که اطلاعات فراهم شده نیازمندیهای مربوط به مفاهیم و ارایه شواهد مرتبط را برآورده می‌کند. - در بخش مرجع سند هدف امنیتی، نسخه‌ی سند هدف امنیتی و تاریخ انتشار آن به درستی ذکر نشده است. نسخه محصول در بخش سند هدف ارزیابی با نسخه درج شده در پانویس سند یکسان نیست.
۵		ASE_TSS.1.1E	ارزیاب باید تایید کند که اطلاعات فراهم شده نیازمندیهای مربوط به مفاهیم و ارایه شواهد مرتبط را برآورده می‌کند. - شرح خلاصه‌ای از هدف ارزیابی که چگونگی برآورده‌سازی هریک از الزامات کارکردی امنیتی SFR را مشخص می‌کند، به صورت کامل ذکر نشده است و تمامی الزامات را پوشش نمی‌دهد.
۶	آزمون‌ها(ATE)	ATE_IND.1.2E	ارزیاب می‌بایست زیرمجموعه‌ای از توابع امنیتی TOE را مورد آزمون قرار دهد و تائید نماید که توابع امنیتی هدف ارزیابی به صورت مشخص شده عمل می‌نمایند. - انطباق نتایج آزمون با نتایج مورد انتظار مورد بررسی قرار گرفت. تمامی الزام‌های کارکردی امنیت پروفایل حفاظتی مربوطه پیاده سازی نشده و یا به صورت صحیح پیاده‌سازی نشده‌اند.

ردیف	کلاس عدم انطباق	نام و شماره بند استاندارد	شرح عدم انطباق
			- تمامی الزام‌های کارکردی امنیت پروفایل حفاظتی مربوطه در سامانه پیاده سازی نشده و یا به صورت صحیح پیاده‌سازی نشده‌اند. (ATE_IND.1-7)

۲-۳- توصیه‌های امنیتی

- در الزام FAU_SAR.3.1 مربوط به موارد مرتب‌سازی و فیلترینگ رویدادهای ممیزی (FAU_SAR.3)موارد زیرتوصیه می شود:
  - امکان فیلتر رویدادهای ممیزی بر اساس نوع رویداد(نوع عملیات) انجام بگیرد.
  - در فیلد نام کاربری به جای ذخیره نام ونام خانوادگی، نام کاربری یا شناسه کاربری، ذخیره گردد.
  - در امکان فیلتر رویدادهای ممیزی به جای فیلتر براســـاس نام یا نام خانوادگی، بر اســـاس نام کاربری فیلتر نماید.

۳- جداول نتایج ارزیابی

دو جدول زیر نمایانگر نتایج آزمون‌های صورت گرفته در فاز اول بر روی سامانه‌ی سیستم یکپارچه شهرسازی آمارد نسخه‌ی1401.03.21.01 متعلق به شرکت تحلیل گران آمارد نوین است.

۳-۱- جدول آزمون‌های SFR[1]s

این بخش با توجه به الزامات عملکردی- امنیتی(SFRs)، در تمامی سطوح تضمین (EAL1-7) استاندارد CC لحاظ شده است. دستورالعمل‌ها و خط‌مشی آزمون براساس متدولوژی CEM تهیه و تدوین شده است.

جدول۱-۳: لیست آزمون‌های انجام شده حوزه SFR

ردیف	عنوان کلاس	وزن	تعداد کل شاخص‌ها	تعداد موارد آزمون شده	تعداد آزمون‌های موفق	درصد انطباق
۱	کلاس ممیزی امنیت	۴	۱۲	۱۲	۳	۲۵.۰۰
۲	کلاس پشتیبانی از رمزنگاری	۴	۹	۵	۰	۰۰.۰۰
۳	کلاس شناسایی و احراز هویت	۴	۱۷	۱۲	۴	۳۳.۳۳
۴	کلاس حفاظت از داده‌های کاربری	۴	۱۷	۱۶	۹	۵۶.۲۵
۵	کلاس مدیریت امنیت	۴	۹	۹	۸	۸۸.۸۹
۶	کلاس حفاظت از توابع امنیتی هدف ارزیابی	۴	۷	۵	۴	۸۰.۰۰
۷	کلاس تخصیص منابع	۴	۱	۱	۱	۱۰۰
۸	کلاس دسترسی به هدف ارزیابی	۴	۸	۸	۴	۵۰.۰۰
۹	کلاس کانال‌ها و مسیرهای مورد اعتماد	۴	۶	۵	۲	۴۰.۰۰
نتیجه نهایی ارزیابی SFRs		انطباق با **۴۷.۹۵ درصد** از الزامات بخش دو استاندارد ISO/IEC/ISIRI 15408				

[1] Security Functional Requirements

۳-۲- جدول آزمون‌های SAR[1]s

این بخش با توجه به الزامات سطح تضمین EAL[2]1 بخش سه استاندارد ISO/IEC/ISIRI 15408 لحاظ شده است. دستورالعمل‌ها و خط‌مشی آزمون براساس متدولوژی CEM تهیه و تدوین شده است.

جدول۲-۳: لیست آزمون‌های انجام شده حوزه SAR

ردیف	عنوان کلاس	نام خانواده	شناسه مؤلفه
۱	کلاس تولید و توسعه (ADV)	خصوصیات عملکردی	ADV_FSP.1
۲	کلاس اسناد راهنما (AGD)	راهنمای عملی کاربر	AGD_OPE.1
۳		رویه‌های تدارک	AGD_PRE.1
۴	کلاس پشتیبانی از چرخه حیات(ALC)	قابلیت‌های مدیریت پیکربندی	ALC_CMC.1
۵		مدیریت پیکربندی	ALC_CMS.1
۶	کلاس ارزیابی هدف امنیتی(ASE)	ادعای انطباق	ASE_CCL.1
۷		تعریف مؤلفه‌های توسعه یافته	ASE_ECD.1
۸		معرفی هدف امنیتی	ASE_INT.1
۹		اهداف امنیتی	ASE_OBJ.1
۱۰		الزامات امنیتی	ASE_REQ.1
۱۱		خلاصه خصوصیات محصول	ASE_TSS.1
۱۲	کلاس آزمون‌ها(ATE)	آزمون مستقل	ATE_IND.1
۱۳	کلاس ارزیابی آسیب‌پذیری(AVA)	تحلیل آسیب‌پذیری	AVA_VAN.1
نتیجه نهایی ارزیابی SARs		**عدم انطباق** با الزامات بخش سه استاندارد ISO/IEC/ISIRI 15408	

[1] Security Assurance Requirements
[2] Evaluation Assurance Level

۴- نتیجه‌گیری

طی آزمون‌های انجام شـــده مطابق با جداول بخش ســـه از این ســـند، نتیجه **فاز اول** ارزیابی ســـامانه‌ی یکپارچه شـهرسـازی آمارد نسـخه‌ی 1401.03.21.01 متعلق به شـرکت تحلیل گران آمارد نوین با قابلیت‌های آورده شـده در جدول ۱-۱- این سند، به شرح ذیل می باشد. مراجعه و استناد به گزارش ۴۹ صفحه‌ای عدم انطباق حاضر و نامه نتیجه روی آزمون جهت بررسی ضرورت دارد.

جدول۱-۴: نتیجه فاز اول ارزیابی سامانه‌ی یکپارچه شهرسازی آمارد

ردیف	
۱	انطباق با **۴۷.۹۵ درصد** از الزامات بخش دو استاندارد ISO/IEC/ISIRI 15408
۲	**عدم انطباق** با الزامات بخش سه استاندارد ISO/IEC/ISIRI 15408

تبصره: جدول فوق نشان دهنده میزان انطباق محصول مذکور در سه حوزه ی SFR ، SAR، الزامات ASVS و همچنین تعیین میزان آسیب پذیری محصول است. نتایج فوق به منزله تایید و گواهی محصول نبوده و سوء استفاده از نتایج آزمایشگاهی قبل از تایید و اعطای گواهی پیگرد قانونی دارد.

۵- محدودیت‌ها و فرضیات ارزیابی

در این بخش کلیه بندهایی که به دلیل محدودیت‌های موجود مورد آزمون واقع نشـــده‌لند و یا در مورد محصـــول کاربرد ندارند، آورده شده‌اند.

جدول۱-۵: محدودیت‌های الزامات کارکرد امنیتی در استاندارد ISO/IEC 15408

ردیف	عنوان کلاس	مؤلفه امنیتی	شرح محدودیت
۱	پشتیبانی از رمزنگاری	FCS_TLSC_EXT.1.1 (SMS Server)	محصول باید TLSv1.2 را با پشتیبانی از مجموعه‌های رمزهای مجاز مندرج در پروفایل حفاظتی پیاده‌سازی نماید. با توجه به اینکه سامانه سیستم یکپارچه شهرسازی آمارد، قادر به ارسال پیامک بر روی https نمی باشد و با عطف به الزام FTP_ITC.1.1(SMS)، لذا الزام در محدودیت ارزیابی قرار می گیرد.
۲		FCS_TLSC_EXT.1.2 (SMS Server)	اگر DN موجود در یک گواهی‌نامه مطابق با DN مورد انتظار برای همتا نباشد، محصول نباید کانال مورد اعتماد را برقرار نماید. عطف به توضیحات الزام FCS_TLSC_EXT.1.1(SMS)، این الزام در ارزیابی جاری قابل بررسی نبوده و در قالب محدودیت‌های ارزیابی اعلام شده است.
۳		FCS_TLSC_EXT.1.3 (SMS Server)	توابع امنیتی هدف ارزیابی باید تنها در صورتی یک کانال مورد اعتماد برقرار نماید که گواهی همتا (peer certificate) معتبر باشد. عطف به توضیحات الزام FCS_TLSC_EXT.1.1(SMS)، این الزام در ارزیابی جاری قابل بررسی نبوده و در قالب محدودیت‌های ارزیابی اعلام شده است.
۴		FCS_TLSC_EXT.4.1 (SMS Server)	محصول باید Supported Elliptic Curves Extension را به همراه NIST curve های • secp256r1 • secp384r1 • secp521r1 یا هیچ گزینه دیگری در پیام ClientHello ارائه دهد.

ردیف	عنوان کلاس	مؤلفه امنیتی	شرح محدودیت
			عطف به توضیحات الزام FCS_TLSC_EXT.1.1(SMS)، این الزام در ارزیابی جاری قابل بررسی نبوده و در قالب محدودیت‌های ارزیابی اعلام شده است.
۵	شناسایی و احراز هویت	FIA_USB.1.2	توابع امنیتی هدف ارزیابی باید قوانین زیر را بر روی ارتباط و پیوند اولیه کاربر فعال اعمال نماید: • زمانیکه یک نشست جدید باید برقرار شود، اطلاعات موجود از نشست‌های قبلی باید حذف گردد. • اطلاعات پیشینه احراز هویت باید بروزرسانی گردد. چون قوانین الزام برای محصول کاربرد ندارد، بنابراین قابلیت تست وجود ندارد، لذا الزام در محدودیت ارزیابی قرار می گیرد.
۶		FIA_X509_EXT.1.1 (SMS Server)	محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین آورده شده در پروفایل حفاظتی مرجع تأیید نماید. با توجه به اینکه سامانه سیستم یکپارچه شهرسازی آمارد، قادر به ارسال پیامک بر روی https نمی باشد و با عطف به الزام FTP_ITC.1.1(SMS)، لذا الزام در محدودیت ارزیابی قرار می گیرد.
۷		FIA_X509_EXT.1.2 (SMS Server)	محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد. عطف به توضیحات الزام FIA_X509_EXT.1.1(SMS Server)، این الزام در ارزیابی جاری قابل بررسی نبوده و در قالب محدودیت‌های ارزیابی اعلام شده است.

ردیف	عنوان کلاس	مؤلفه امنیتی	شرح محدودیت
۸		FIA_X509_EXT.2.1 (SMS Server)	محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای TLS, HTTPS و امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم، امضای کد برای تأیید یکپارچگی، سایر کاربردهای دیگر از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند. عطف به توضیحات الزام FIA_X509_EXT.1.1(SMS Server)، این الزام در ارزیابی جاری قابل بررسی نبوده و در قالب محدودیت‌های ارزیابی اعلام شده است.
۹		FIA_X509_EXT.2.2 (SMS Server)	وقتی تابع امنیتی هدف ارزیابی نتواند ارتباطی ایجاد کند تا اعتبار یک گواهینامه را بسنجد، تابع امنیتی هدف ارزیابی باید یکی از اقدامات زیر را انجام دهد: • به سرپرست اجازه دهد انتخاب کند که در این موارد گواهینامه را بپذیرد. • گواهینامه را بپذیرد. • گواهینامه را نپذیرد. عطف به توضیحات الزام FIA_X509_EXT.1.1(SMS Server)، این الزام در ارزیابی جاری قابل بررسی نبوده و در قالب محدودیت‌های ارزیابی اعلام شده است.
۱۰	حفاظت از داده‌های کاربری	FDP_ITC.2.5	توابع امنیتی هدف ارزیابی باید در هنگام ورود داده کاربری تحت کنترل خط‌مشی امنیتی از خارج هدف ارزیابی، قوانین زیر را اعمال نماید: با توجه به آنکه امضای دیجیتال داده‌های کاربری در هنگام ورود داده در سامانه‌های تحت وب می‌تواند به عنوان مشخصه‌های امنیتی آن داده‌ها به شمار رود و در این سامانه برای ورود داده‌ها و آپلود فایل‌ها توسط کاربران از امضای دیجیتال بهره گرفته نمی‌شود، الزام برای محصول کاربر ندارد.

ردیف	عنوان کلاس	مؤلفه امنیتی	شرح محدودیت
۱۱	حفاظت از توابع امنیتی هدف ارزیابی	FPT_TUD_EXT.1.2	محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی فراهم کند که به‌روزرسانی نرم‌افزار و میان‌افزار محصول مورد ارزیابی را به صورت دستی آغاز نماید و - از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند یا - از به‌روزرسانی‌های خودکار پشتیبانی کند یا - از هیچ مکانیزم به‌روزرسانی دیگری پشتیبانی نکند. قابلیتی مبنی بر به روز رسانی خودکار در سامانه مشاهده نشد. علاوه بر این این الزام در سند پروفایل حفاظتی مرجع وجود نداشته و برای سامانه‌های تحت وب مورد ارزیابی بر اساس پروفایل حفاظتی برنامه کاربردی تحت شبکه قابل ارزیابی نیست و در محدودیت قرار می‌گیرد.
۱۲		FPT_TUD_EXT.1.3	توابع امنیتی هدف ارزیابی باید به وسیله روشی قبل از به‌روزرسانی هدف ارزیابی، با استفاده از سازو کارهای امضای دیجیتال یا مقادیر درهم‌سازی منتشر شده از صحت به‌روزرسانی نرم افزاری/میان افزاری اطمینان حاصل کنند. قابلیتی مبنی بر به روز رسانی خودکار در سامانه مشاهده نشد. علاوه بر این این الزام در سند پروفایل حفاظتی مرجع وجود نداشته و برای سامانه‌های تحت وب مورد ارزیابی بر اساس پروفایل حفاظتی برنامه کاربردی تحت شبکه قابل ارزیابی نیست و در محدودیت قرار می‌گیرد.
۱۳	کانال ها و مسیرهای مطمئن	FTP_ITC.1.2 (SMS)	محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند. با توجه به اینکه امکان برقراری ارتباط از طریق موجودیت معتبر IT با سامانه وجود ندارد، ارزیابی این الزام در محدودیت قرار می‌گیرد.

جدول۲-۵: محدودیت‌های الزامات تضمین امنیت در استاندارد ISO/IEC 15408

ردیف	عنوان کلاس	مؤلفه امنیتی	شرح محدودیت
۱	ارزیابی هدف امنیتی	AVA_VAN.1.3E	ارزیاب براساس آسیب پذیریهای بالقوه شناسایی شده آزمون های تست نفوذ متناسب با آنها را اعمال نماید تا تعیین کند که محصول در برابر حملات بالقوه مقاوم است. نظر به عدم تکمیل آزمون‌های ارزیابی آسیب‌پذیریدر فاز اول ارزیابی، این الزام در محدودیت ارزیابی قرار می گیرد.