

به نام خدا

سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

شرکت رسانه ساز دانش

سامانه ساز جامع آریو

۲۰,۳۴۱



آذر ماه ۱۴۰۱

نسخه ۱,۸

پیشگفتار

در نظام ارزیابی امنیتی محصولات فتا، یکی از اسناد مورد نیاز برای انجام آزمون امنیتی، سند هدف امنیتی است. بر اساس استاندارد معیار مشترک (CC) سند هدف امنیتی مبتنی بر اسنادی که پروفایل حفاظتی نام دارند، تهیه و تدوین می‌گردد. پروفایل‌های حفاظتی حاوی الزامات امنیتی هستند که در یک محصول افتایی می‌بایست رعایت گردد. از آنجا که متن این پروفایل‌ها پیچیده بوده، تهیه سند هدف امنیتی برای تولیدکننده کاری زمان‌بر است، ساده‌سازی الزامات امنیتی موجود در پروفایل‌های حفاظتی به نحوی که برای تولیدکننده مشخص شود که چه مواردی امنیتی باید در یک محصول خاص رعایت شود، بسیار مفید خواهد بود.

در این راستا مرکز افتا و سازمان فناوری اطلاعات ایران با همکاری آزمایشگاه‌های ارزیابی امنیتی، به منظور چابک‌سازی فرآیند ارزیابی امنیتی، «سند الزامات امنیتی» را جایگزین پروفایل‌های حفاظتی نموده است. هدف از سند الزامات امنیتی، ساده‌سازی مفاهیم الزامات مطرح شده در پروفایل‌های حفاظتی و نیز کمک به تولیدکننده در جهت سرعت بخشیدن به تدوین سند هدف امنیتی است.

سند پیشرو حاوی الزامات امنیتی «پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه» که سعی شده است تا حد ممکن ساده و قابل فهم گردد، است. این سند دو هدف را دنبال می‌کند. اول آنکه موارد امنیتی را که باید در محصول رعایت شود (تا منجر به دریافت گواهی امنیتی گردد) برای تولیدکننده مشخص نماید و ثانیاً، تدوین سند هدف امنیتی را که کاری زمان‌بر است را برای تولیدکننده سریع و آسان نماید.

فهرست

| | |
|-------------------------------------|----------------------------------|
| ۳ | فهرست |
| ۱- مقدمه | Error! Bookmark not defined..... |
| ۲- الزامات امنیتی | ۵..... |
| ۲-۱- ممیزی امنیت (لاگ) | ۵..... |
| ۲-۲- رمزنگاری | ۹..... |
| ۲-۳- شناسایی و احراز هویت | ۱۱..... |
| ۲-۴- حفاظت از داده‌ی کاربری | ۱۵..... |
| ۲-۵- مدیریت امنیت | ۱۹..... |
| ۲-۶- حفاظت از توابع امنیتی محصول | ۲۲..... |
| ۲-۷- تخصیص منابع | ۲۴..... |
| ۲-۸- دسترسی به محصول | ۲۵..... |
| ۲-۹- کانال‌ها/مسیرهای مورد اعتماد | ۲۷..... |
| ۳- الزامات امنیتی مبتنی بر انتخاب | ۲۸..... |
| ۳-۱- پروتکل HTTPS | ۲۸..... |
| ۳-۲- پروتکل TLS Client | ۲۹..... |
| ۳-۳- پروتکل TLS Server | ۳۳..... |
| ۳-۴- پروتکل TLS مشترک کلاینت و سرور | ۳۵..... |
| ۳-۵- اعتبارسنجی گواهی‌نامه | ۳۶..... |
| ۳-۶- پروتکل SSH | ۳۸..... |

۱- معرفی محصول

سیستم ساز آریو شامل (سامانه مدیریت فرآیند سازمانی، موجودیت و فرم ساز، گزارش ساز و داشبوردساز) با جدیدترین تکنولوژی های صنعت آی تی، طراحی و تولید شده تا سازمانها را در تهیه سامانه ها مطابق با نیاز خود یاری رساند. سیستم ساز آریو ابزاری است جهت کاهش هزینه و تسریع در رسیدن به سامانه های اطلاعاتی مطابق با نیاز و الگوی سازمان با کمترین هزینه که می توان بواسطه آن سامانه های اطلاعاتی و نرم افزارهای کاربردی مطابق با نیاز سازمان را ایجاد نمود و سازمان را به سمت توانمندتر شدن در ارائه محصولات و خدمات سوق داد.

سازمان ها با استفاده از این ابزار می توانند:

الف) فرم های عملیاتی خود را توسط فرم ساز در کمترین زمان ممکن و به آسانی طراحی و تولید نمایند.

ب) فرآیند کاری خود را با فرایند ساز بصورت بصری بسازند و با هر تغییر به روز نمایند.

ج) گزارشات و داشبوردهای مورد نیاز خود را توسط ابزار گزارش ساز طراحی کنند.

اجزا اصلی سامانه آریو:

- موجودیت ساز و فرمساز (Form Generator)
- گزارش ساز (Report Generator)
- داشبورد ساز و هوش تجاری (BI)
- زیر سامانه مدیریت فرآیندها (BPMS Engine)
- زیر سامانه مدیریت دسترسی ها (Security Service)
- زیر سامانه مدیریت میز کار
- زیر سامانه مدیریت کار تابل

۲- الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه ۱,۱ نمایه^۱ حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر رده در پروفایل حفاظتی مربوطه، یک دسته الزام بیان شده است.

۲-۱- ممیزی امنیت (Log)

در این رده توانایی‌های محصول از نظر امکان تولید داده ممیزی (Log) مناسب برای فعالیت‌های مختلفی که در محصول صورت می‌گیرد، در شرایط مختلف سنجیده می‌شود.

| توضیحات | رده ممیزی امنیت (Log) | شماره الزام |
|---------|--|--|
| | <input checked="" type="checkbox"/> محصول باید برای موارد مشخص شده که در زیر آمده است، ثبت‌نشان ^۲ تولید کند (Log) ثبت نماید). | ۱ |
| | <input checked="" type="checkbox"/> شروع و اتمام توابع | رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید. |
| | <input checked="" type="checkbox"/> تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها | |
| | <input checked="" type="checkbox"/> خواندن اطلاعات از ثبت‌نشان‌ها | |
| | <input checked="" type="checkbox"/> تمامی تغییرات در پیکربندی ثبت‌نشان‌ها | |
| | <input checked="" type="checkbox"/> عملیات انجام شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه | |
| | <input checked="" type="checkbox"/> عملیات انجام شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها | |
| | <input checked="" type="checkbox"/> تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی. | |
| | <input checked="" type="checkbox"/> تمام کاربردهای سازوکار احراز هویت | |
| | <input checked="" type="checkbox"/> نتایج نهایی عملیات احراز هویت | |
| | <input checked="" type="checkbox"/> تلاش موفق و ناموفق هر گذرواژه بررسی شده توسط محصول | |

^۱ Profile

^۲ Log

| | | | |
|--|-------------------------------------|--|--|
| | <input checked="" type="checkbox"/> | شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال) | |
| | <input checked="" type="checkbox"/> | تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی | |
| | <input checked="" type="checkbox"/> | تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول | |
| | <input checked="" type="checkbox"/> | تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی) | |
| | <input checked="" type="checkbox"/> | همه تلاش‌ها برای خارج کردن اطلاعات از محصول | |
| | <input checked="" type="checkbox"/> | تمامی تغییرات در رفتارهای توابع کارکردی محصول | |
| | <input checked="" type="checkbox"/> | استفاده از کارکردهای مدیریتی | |
| | <input checked="" type="checkbox"/> | تغییرات در گروه کاربران | |
| | <input checked="" type="checkbox"/> | شکست در کارکردهای امنیتی محصول | |
| | <input checked="" type="checkbox"/> | تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند. | |
| | <input checked="" type="checkbox"/> | تلاش موفق یا ناموفق برای برقراری نشست. | |
| | <input checked="" type="checkbox"/> | ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل) | |
| | <input checked="" type="checkbox"/> | خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست | |
| | <input type="checkbox"/> | خاتمه به نشست غیرفعال توسط مدیر سیستم | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید. | ۲ |
| | <input checked="" type="checkbox"/> | تاریخ و زمان رویداد | و ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود. |
| | <input checked="" type="checkbox"/> | نوع رویداد | |
| | <input checked="" type="checkbox"/> | هویت ایجادکننده رویداد | |
| | <input checked="" type="checkbox"/> | نتیجه رویداد | |
| | <input checked="" type="checkbox"/> | آدرس IP ایجادکننده رویداد | |

| | | | |
|--|-------------------------------------|---|---|
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید. | |
| | <input checked="" type="checkbox"/> | ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند. | |
| | <input checked="" type="checkbox"/> | نبود داده نامفهوم در رکوردها | مواردی که در |
| | <input checked="" type="checkbox"/> | نبود بخش‌های نامرتب | ثبت‌نشان‌ها وجود |
| | <input checked="" type="checkbox"/> | وجود داده معتبر و مناسب در هر بخش | دارند، مشخص شوند. |
| | <input checked="" type="checkbox"/> | محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید. | |
| | <input checked="" type="checkbox"/> | هویت موجودیت فعال | مواردی که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود. |
| | <input checked="" type="checkbox"/> | نوع حساب کاربری | |
| | <input checked="" type="checkbox"/> | تاریخ‌ازمان | |
| | <input checked="" type="checkbox"/> | روش اتصال کاربر | |
| | <input checked="" type="checkbox"/> | نوع رخداد | |
| | <input checked="" type="checkbox"/> | مکان رویداد | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید. | |
| | <input type="checkbox"/> | استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات | روش‌های تشخیص |
| | <input checked="" type="checkbox"/> | پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری) | مشخص شود. (وجود) |
| | <input checked="" type="checkbox"/> | فقط خواندنی کردن ثبت‌نشان‌ها در محصول | یک مورد لازم و کافی |
| | <input type="checkbox"/> | سایر موارد | (است) |

| | | | |
|--|-------------------------------------|--|-----------------------------------|
| | <input checked="" type="checkbox"/> | <p>۷ محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.</p> | |
| | <input type="checkbox"/> | استفاده از یک کانال ارتباطی | روش‌های اطلاع‌رسانی |
| | <input type="checkbox"/> | ارسال پیام | مشخص شود (وجود) |
| | <input checked="" type="checkbox"/> | از طریق واسط کاربر مجاز | یک مورد لازم و کافی |
| | <input type="checkbox"/> | سایر موارد | (است) |
| | <input checked="" type="checkbox"/> | <p>۸ محصول باید توانایی تولید ثبت‌نشان (ثبت Log) هنگام از کار افتادن محصول و/یا پر شدن حافظه ثبت‌نشان‌ها را داشته باشد و برای این کار از رویکردهای بیان‌شده استفاده نماید.</p> | |
| | <input type="checkbox"/> | نادیده گرفتن ثبت‌نشان‌ها | رویکرد های مورد |
| | <input type="checkbox"/> | ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهايي که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند) | استفاده در محصول مشخص گردد (وجود) |
| | <input checked="" type="checkbox"/> | بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده | یک مورد لازم و کافی |
| | <input type="checkbox"/> | سایر موارد | (است) |

۲-۲- رمزنگاری

در این رده، توانایی محصول در پیاده‌سازی یا به‌کارگیری ماژولهای رمزنگاری، بررسی می‌گردد. برای حفظ محرمانگی داده از رمزنگاری استفاده می‌گردد و این رمزنگاری‌ها می‌تواند به صورت متقارن و نامتقارن صورت گیرد. در رمزنگاری متقارن از یک کلید مشترک برای رمزگذاری و رمزگشایی، استفاده می‌شود ولی در رمزنگاری نامتقارن این کار با استفاده از یک زوج کلید (کلید عمومی و کلید خصوصی) صورت می‌گیرد. الگوریتمها میتوانند با طول کلیدهای مختلف و به روشهای مختلفی (مد عملیاتی) به رمزگذاری و رمزگشایی داده بپردازند که در این رده، توانایی محصول از این حیث مورد بررسی قرار گرفته است. در رده رمزنگاری همچنین از الگوریتمهای درهم‌سازی (هش) برای برقراری جامعیت داده استفاده می‌گردد.

| شماره الزام | رده رمزنگاری | توضیحات |
|-------------|--|---|
| ۱ | <input checked="" type="checkbox"/> محصول باید قابلیت رمزنگاری یا واحد ^۲ رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف شده ISO 18033-3) با توجه به موارد زیر انجام دهد. | <input type="checkbox"/> مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در (NIST SP 800-38A) از آن استفاده می‌کند را انتخاب نماید. (وجود یک مورد لازم و کافی است.) |
| | | <input checked="" type="checkbox"/> مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در (NIST SP 800-38D) |
| | | <input type="checkbox"/> مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در (ISO10116) |
| | | <input checked="" type="checkbox"/> محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (Hash) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید. |
| ۲ | <input type="checkbox"/> الگوریتم و اندازه خلاصه الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰ بیت | <input checked="" type="checkbox"/> الگوریتم و اندازه خلاصه پیام مورد استفاده را الگوریتم SHA-256 با اندازه خلاصه پیام ۲۵۶ بیت |

^۲ Module

| | | | |
|--|-------------------------------------|--|--|
| | <input checked="" type="checkbox"/> | الگوریتم SHA-384 با اندازه خلاصه پیام ۳۸۴ بیت | انتخاب نمایید. (وجود |
| | <input type="checkbox"/> | الگوریتم SHA-512 با اندازه خلاصه پیام ۵۱۲ بیت | یک مورد لازم و کافی است.) |
| | <input checked="" type="checkbox"/> | در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری) | |
| | <input type="checkbox"/> | نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یک‌ها، مقدار تصادفی، مقدار جدیدی از کلید) | روش نابودی کلید مشخص گردد. (وجود |
| | <input type="checkbox"/> | نابودی با استفاده از یک واسط مشخص | یک مورد لازم و کافی است) |
| | <input checked="" type="checkbox"/> | از طریق توابع امنیتی محصول | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | در صورتی که امضای دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضای رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری) | |
| | <input checked="" type="checkbox"/> | الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS) بخش ۵،۵، | الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. |
| | <input checked="" type="checkbox"/> | الگوی امضای RSASSA-PSS نسخه ۲.۱ v2.1 PKCS #1 و یا RSASSA-ISO/IEC 9796-2؛ PKCS1v_5، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال (۳) | |
| | <input checked="" type="checkbox"/> | الگوریتم‌های امضای دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵۶ بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش ۴،۶، استاندارد امضای دیجیتال (DSS) بخش ۶ و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521) | (وجود یک مورد لازم و کافی است) |

۲-۳- شناسایی و احراز هویت

در این رده توانایی‌های محصول از نظر امکان شناسایی و احراز هویت کاربر در حالت‌های مختلف و اقدامات متقابل در راستای عدم برقراری آنها، بررسی می‌گردد.

| توضیحات | رده شناسایی و احراز هویت | | شماره الزام |
|---------|-------------------------------------|---|---|
| | <input checked="" type="checkbox"/> | محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید. | ۱ |
| | <input type="checkbox"/> | یک عدد مثبت ثابت | مقدار یا یازهی مورد استفاده در هریک باید |
| | <input checked="" type="checkbox"/> | یک عدد مثبت قابل تنظیم توسط مدیر | مشخص گردد. (وجود |
| | <input type="checkbox"/> | یک بازهی قابل قبولی از مقادیر | یک مورد لازم و کافی (است) |
| | <input checked="" type="checkbox"/> | محصول باید زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید. | |
| | <input checked="" type="checkbox"/> | غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد) | روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب |
| | <input checked="" type="checkbox"/> | غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد) | نمایید. (وجود یک مورد لازم و کافی است). لازم به ذکر است روش‌های فوق با توجه |
| | <input type="checkbox"/> | استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود) | به نوع کاربرد می‌تواند از حالت انتخایی به حالت الزامی تغییر یابد. |

| | | | |
|--|-------------------------------------|---|---|
| | <input type="checkbox"/> | سایر موارد | برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست. |
| | <input checked="" type="checkbox"/> | <p>۳ محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید.</p> | |
| | <input checked="" type="checkbox"/> | شناسه کاربر | ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند. |
| | <input checked="" type="checkbox"/> | روش احراز هویت مورد استفاده | |
| | <input checked="" type="checkbox"/> | داده احراز هویت | |
| | <input checked="" type="checkbox"/> | وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره) | |
| | <input checked="" type="checkbox"/> | نقش کاربر | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | <p>۴ محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.</p> | |
| | <input checked="" type="checkbox"/> | استفاده از حروف کوچک | موارد نیاز که باید در تعریف گذرواژه استفاده شوند. |
| | <input checked="" type="checkbox"/> | استفاده از حروف بزرگ | |
| | <input checked="" type="checkbox"/> | استفاده از اعداد | |
| | <input checked="" type="checkbox"/> | استفاده از کاراکترهای خاص (@, #, \$, %, ^, &, * و ...) | |
| | <input checked="" type="checkbox"/> | حداقل طول ۸ یا بیشتر (قابل تنظیم) | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | <p>۵ محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.</p> | |
| | <input type="checkbox"/> | مشاهده راهنمای نحوه ورود به سیستم | اقدامات عمومی که |
| | <input checked="" type="checkbox"/> | بازیابی گذرواژه | کاربر می‌تواند قبل از |

| | | | |
|---|-------------------------------------|---|--|
| | <input type="checkbox"/> | هیچ اقدامی | احراز هویت انجام دهد، |
| | <input checked="" type="checkbox"/> | سایر موارد | انتخاب شود. |
| ۶ | <input checked="" type="checkbox"/> | محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد). | |
| | <input checked="" type="checkbox"/> | نام کاربری و گذرواژه | سازوکارهای احراز هویت موجود در محصول مشخص شوند. |
| | <input type="checkbox"/> | امضای دیجیتال | |
| | <input checked="" type="checkbox"/> | Active Directory | |
| | <input type="checkbox"/> | OTP یا توکن | |
| | <input checked="" type="checkbox"/> | احراز هویت دو فاکتوری | |
| | <input type="checkbox"/> | سایر موارد | |
| ۷ | <input checked="" type="checkbox"/> | محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید. | |
| | <input checked="" type="checkbox"/> | شناسه کاربر | ویژگی‌هایی امنیتی که محصول برای هر کاربر نگهداری می‌کند، |
| | <input checked="" type="checkbox"/> | نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه | مشخص گردد (در صورتی که محصول قوانین بیشتری هنگام |
| | <input type="checkbox"/> | جزئیات واسط کلاینت | برقراری نشست اعمال می‌نماید، این قوانین |
| | <input checked="" type="checkbox"/> | پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق) | در «سایر موارد» بیان می‌شوند). |
| | <input type="checkbox"/> | سایر موارد | |
| ۸ | <input checked="" type="checkbox"/> | محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید. | |

| | | | |
|--|-------------------------------------|--|--|
| | <input checked="" type="checkbox"/> | از بین رفتن اعتبار نشستهای قبلی هنگام برقراری یک نشست جدید (به جز مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشست‌های جدید، باید به صفحه کاربر اصلی (نشست اول) اطلاع داده شود). | در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند). |
| | <input checked="" type="checkbox"/> | بروزرسانی اطلاعات پیشینه احراز هویت | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید. | |
| | <input checked="" type="checkbox"/> | غیرمجاز بودن هرگونه تغییر در طول نشست فعال | قوانینی که در صورت تغییر ویژگی‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد. |
| | <input type="checkbox"/> | سایر موارد | |

۴-۲- حفاظت از داده‌ی کاربری

داده کاربری در واقع هر نوع داده‌ای است که کاربر تولید می‌کند یا مالک آن است. توضیح کامل داده کاربری در سند «راهنمای سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه» در قسمت اصطلاحات بیان گردیده است. در این رده، توانایی محصول در حفاظت از این داده‌ها مورد بررسی قرار می‌گیرد.

| توضیحات | رده حفاظت از داده‌ی کاربری | | شماره الزام |
|---------|--|--|-------------|
| | محصول باید برای موجودیت‌ها و عملیات، خطمشی‌های کنترل دسترسی اعمال نماید. | | ۱ |
| | <input checked="" type="checkbox"/> | مدیر سیستم موجودیت‌های فعالی که خطمشی‌های | |
| | <input checked="" type="checkbox"/> | کاربر عادی کنترل دسترسی در مورد آنها اعمال | |
| | <input type="checkbox"/> | سایر موارد می‌شوند، مشخص گردد. | |
| | <input checked="" type="checkbox"/> | سوابق، مستندات و فراداده موجودیت‌های غیرفعال | |
| | <input checked="" type="checkbox"/> | داده متعلق به کاربران که خطمشی‌های کنترل دسترسی در | |
| | <input checked="" type="checkbox"/> | داده احراز هویت مورد آنها اعمال | |
| | <input type="checkbox"/> | سایر موارد می‌شوند، مشخص گردد. | |
| | <input checked="" type="checkbox"/> | ایجاد موجودیت غیرفعال جدید عملیاتی که | |
| | <input checked="" type="checkbox"/> | حذف موجودیت غیرفعال خطمشی‌های کنترل | |
| | <input checked="" type="checkbox"/> | تغییر دسترسی‌ها به موجودیت غیرفعال دسترسی در رابطه با | |
| | <input checked="" type="checkbox"/> | عملیات بر روی فراداده وابسته به موجودیت غیرفعال | |

| | | | |
|--|-------------------------------------|---|--|
| | <input type="checkbox"/> | سایر موارد | آنها اعمال می‌شوند، مشخص گردد. |
| | <input type="checkbox"/> | محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید. | |
| | <input checked="" type="checkbox"/> | نقش‌ها و مجوزهای کاربر مجاز | و ویژگی‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند، |
| | <input type="checkbox"/> | اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند. | انتخاب گردد. |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در لیست کنترل دسترسی، سابقه (رکوردی) وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد). | |
| | <input checked="" type="checkbox"/> | محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید. | |
| | <input checked="" type="checkbox"/> | عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف شده | قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود). |
| | <input checked="" type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام تخصیص و یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد. | |
| | <input checked="" type="checkbox"/> | محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند. | |

| | | | |
|--|-------------------------------------|---|---|
| | <input checked="" type="checkbox"/> | نوع داده | ویژگی‌های امنیتی مرتبط با داده کاربری |
| | <input checked="" type="checkbox"/> | حجم و اندازه | که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص شود |
| | <input checked="" type="checkbox"/> | فرمت | (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد). |
| | <input type="checkbox"/> | تعداد دفعات Import | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | <p>۷ محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفاف را بین داده کاربری دریافت‌شده و ویژگی‌های امنیتی آن فراهم و همچنین از شنود و گم‌شدن داده حین انتقال جلوگیری می‌کند.</p> | |
| | <input checked="" type="checkbox"/> | <p>۸ محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.</p> | |
| | <input checked="" type="checkbox"/> | نوع داده | ویژگی‌های امنیتی مرتبط با داده کاربری |
| | <input type="checkbox"/> | حجم و اندازه | که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند |
| | <input checked="" type="checkbox"/> | فرمت | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | <p>۹ محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.</p> | |

| | | | |
|--|-------------------------------------|--|---|
| | <input checked="" type="checkbox"/> | مدیر سیستم باید خروج داده‌ها را محدود نماید، به طوری‌که کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند. | قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد. | |
| | <input checked="" type="checkbox"/> | مقدار درهم‌سازی‌شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود. | چگونگی تشخیص تغییر در داده‌های کاربری حساس، مشخص شود. |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد. | |
| | <input checked="" type="checkbox"/> | ایجاد هشدار/اخطار برای نقش‌های مجاز | اقدام مقابله‌ای در صورت تشخیص خطا، مشخص شود (وجود) |
| | <input type="checkbox"/> | تصحیح داده بر اساس مقادیر قبل | یک مورد لازم و کافی است) |
| | <input type="checkbox"/> | سایر موارد | |

۲-۵- مدیریت امنیت

در این رده توانایی‌های محصول در مدیریت (حذف، تغییر، فعال کردن و ...) کارکردهای امنیتی (جمع‌آوری داده‌های سیستم، پیکربندی‌ها و ...) مورد بررسی قرار می‌گیرد. همچنین توانایی محصول در مدیریت نقش‌ها و دسترسی آنها برای اعمال مدیریت بر روی کارکردهای امنیتی سنجیده می‌شود.

| توضیحات | رده مدیریت امنیت | شماره الزام | | | | | | | | | | | |
|-------------------------------------|---|---|---------------------|---|-------------------------------------|---------------|-------------------------------------|------------|-------------------------------------|---------------|--------------------------|------------|---|
| | <p><input checked="" type="checkbox"/> محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیت‌های مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.</p> <table border="1" data-bbox="919 651 1948 852"> <tr> <td data-bbox="919 651 961 699"><input checked="" type="checkbox"/></td> <td data-bbox="961 651 1709 699">تعیین و تغییر رفتار</td> <td data-bbox="1709 651 1948 699" rowspan="4">فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.</td> </tr> <tr> <td data-bbox="919 699 961 748"><input checked="" type="checkbox"/></td> <td data-bbox="961 699 1709 748">غیرفعال نمودن</td> </tr> <tr> <td data-bbox="919 748 961 797"><input checked="" type="checkbox"/></td> <td data-bbox="961 748 1709 797">فعال نمودن</td> </tr> <tr> <td data-bbox="919 797 961 852"><input type="checkbox"/></td> <td data-bbox="961 797 1709 852">سایر موارد</td> </tr> </table> | <input checked="" type="checkbox"/> | تعیین و تغییر رفتار | فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند. | <input checked="" type="checkbox"/> | غیرفعال نمودن | <input checked="" type="checkbox"/> | فعال نمودن | <input type="checkbox"/> | سایر موارد | ۱ | | |
| <input checked="" type="checkbox"/> | تعیین و تغییر رفتار | فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند. | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | غیرفعال نمودن | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | فعال نمودن | | | | | | | | | | | | |
| <input type="checkbox"/> | سایر موارد | | | | | | | | | | | | |
| | <p><input checked="" type="checkbox"/> محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام ۷ از رده (Class) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.</p> <table border="1" data-bbox="919 1015 1948 1265"> <tr> <td data-bbox="919 1015 961 1063"><input checked="" type="checkbox"/></td> <td data-bbox="961 1015 1709 1063">پرس‌وجو</td> <td data-bbox="1709 1015 1948 1063" rowspan="5">عملیات بر روی ویژگی‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.</td> </tr> <tr> <td data-bbox="919 1063 961 1112"><input checked="" type="checkbox"/></td> <td data-bbox="961 1063 1709 1112">تغییر</td> </tr> <tr> <td data-bbox="919 1112 961 1161"><input checked="" type="checkbox"/></td> <td data-bbox="961 1112 1709 1161">حذف</td> </tr> <tr> <td data-bbox="919 1161 961 1209"><input checked="" type="checkbox"/></td> <td data-bbox="961 1161 1709 1209">تغییر پیش‌فرض</td> </tr> <tr> <td data-bbox="919 1209 961 1265"><input type="checkbox"/></td> <td data-bbox="961 1209 1709 1265">سایر موارد</td> </tr> </table> | <input checked="" type="checkbox"/> | پرس‌وجو | عملیات بر روی ویژگی‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد. | <input checked="" type="checkbox"/> | تغییر | <input checked="" type="checkbox"/> | حذف | <input checked="" type="checkbox"/> | تغییر پیش‌فرض | <input type="checkbox"/> | سایر موارد | ۲ |
| <input checked="" type="checkbox"/> | پرس‌وجو | عملیات بر روی ویژگی‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد. | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | تغییر | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | حذف | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | تغییر پیش‌فرض | | | | | | | | | | | | |
| <input type="checkbox"/> | سایر موارد | | | | | | | | | | | | |
| | <p><input checked="" type="checkbox"/> محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.</p> <table border="1" data-bbox="919 1382 1948 1424"> <tr> <td data-bbox="919 1382 961 1424"><input checked="" type="checkbox"/></td> <td data-bbox="961 1382 1948 1424">تغییر پیش‌فرض</td> </tr> </table> | <input checked="" type="checkbox"/> | تغییر پیش‌فرض | ۳ | | | | | | | | | |
| <input checked="" type="checkbox"/> | تغییر پیش‌فرض | | | | | | | | | | | | |

| | | | |
|---|--|---|---|
| <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> | حذف نمودن پرس و جو مقاردهی ایجاد مشاهده سایر موارد | عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود. | |
| <input checked="" type="checkbox"/> | محصول باید توانایی انجام کارکردهای زیر را داشته باشد. | | ۴ |
| <input checked="" type="checkbox"/> | پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشده‌ها | در صورتی که هر کدام از موارد مطرح‌شده، توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد. | |
| <input checked="" type="checkbox"/> | پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشده‌ها | | |
| <input checked="" type="checkbox"/> | پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشده‌ها | | |
| <input checked="" type="checkbox"/> | مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول | | |
| <input type="checkbox"/> | انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیگیری باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع) | | |
| <input checked="" type="checkbox"/> | ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول | | |
| <input checked="" type="checkbox"/> | در نظر گرفتن یک عملیات از پیش تعیین‌شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیگیری نیز باشد. | | |
| <input checked="" type="checkbox"/> | ۱. مدیریت حد آستانه برای تلاش‌های ناموفق ۲. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد. | | |
| <input checked="" type="checkbox"/> | مدیریت معیارها برای تنظیم گذرواژه‌ها | | |
| <input checked="" type="checkbox"/> | ۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه ۲. مدیریت یک‌سری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند. | | |

| | | | | | | | | | | | | | | | |
|-------------------------------------|-------------------------------------|---|-------------------------------------|------------|----------------|-------------------------------------|---------------|----------------|-------------------------------------|------------|---------------|--------------------------|------------|-------|---|
| | <input checked="" type="checkbox"/> | <p>۱. مدیریت سازوکارهای احراز هویت</p> <p>۲. مدیریت قوانین مرتبط با احراز هویت</p> | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>مدیریت تغییرات و فرآیندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.</p> | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.</p> | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول</p> | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>مدیریت نقش‌ها در محصول</p> | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر</p> | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>مدیریت شرایط آغاز نشست توسط مدیر مجاز</p> | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>۱. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد.</p> <p>۲. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.</p> | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.</p> <table border="1" data-bbox="961 1015 2030 1214"> <tr> <td data-bbox="961 1015 1711 1068"><input checked="" type="checkbox"/></td> <td data-bbox="1711 1015 2030 1068">مدیر سیستم</td> <td data-bbox="961 1015 1711 1068">نقش‌هایی که در</td> </tr> <tr> <td data-bbox="961 1068 1711 1122"><input checked="" type="checkbox"/></td> <td data-bbox="1711 1068 2030 1122">کاربر پیشرفته</td> <td data-bbox="961 1068 1711 1122">محصول پشتیبانی</td> </tr> <tr> <td data-bbox="961 1122 1711 1175"><input checked="" type="checkbox"/></td> <td data-bbox="1711 1122 2030 1175">کاربر عادی</td> <td data-bbox="961 1122 1711 1175">می‌شوند، مشخص</td> </tr> <tr> <td data-bbox="961 1175 1711 1214"><input type="checkbox"/></td> <td data-bbox="1711 1175 2030 1214">سایر موارد</td> <td data-bbox="961 1175 1711 1214">گردد.</td> </tr> </table> | <input checked="" type="checkbox"/> | مدیر سیستم | نقش‌هایی که در | <input checked="" type="checkbox"/> | کاربر پیشرفته | محصول پشتیبانی | <input checked="" type="checkbox"/> | کاربر عادی | می‌شوند، مشخص | <input type="checkbox"/> | سایر موارد | گردد. | ۵ |
| <input checked="" type="checkbox"/> | مدیر سیستم | نقش‌هایی که در | | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | کاربر پیشرفته | محصول پشتیبانی | | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | کاربر عادی | می‌شوند، مشخص | | | | | | | | | | | | | |
| <input type="checkbox"/> | سایر موارد | گردد. | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>محصول باید قادر باشد کاربران را به نقش‌های تعریف‌شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.</p> | ۶ | | | | | | | | | | | | |

۲-۶- حفاظت از توابع امنیتی محصول

در این رده، توانایی محصول در حفظ وضعیت امن در زمان رخ دادن شکست و همچنین حفاظت از داده‌ها هنگام تبادل بین اجزای محصول یا تبادل با موجودیت‌های دیگر، مورد بررسی قرار گرفته است.

| توضیحات | رده حفاظت از توابع امنیتی محصول | | شماره الزام |
|---------|-------------------------------------|---|---|
| | <input checked="" type="checkbox"/> | محصول باید هنگام رخ دادن هرگونه خرابی، اشکال یا شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته، صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید. | ۱ |
| | <input checked="" type="checkbox"/> | خرابی‌های نرم‌افزاری | هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول |
| | <input checked="" type="checkbox"/> | خرابی‌های سخت‌افزاری | حفظ می‌شود، مشخص گردد. |
| | <input checked="" type="checkbox"/> | محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی جلوگیری از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد. | |
| | <input checked="" type="checkbox"/> | در صورتی که محصول از محصولات امن IT استفاده می‌کند، باید تفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک‌گذاری آن بین خود و دیگر محصولات امن IT، فراهم آورد. | |
| | <input checked="" type="checkbox"/> | داده‌های احراز هویت | داده امنیتی قابل |
| | <input type="checkbox"/> | کلید | اشتراک‌گذاری که در |
| | <input type="checkbox"/> | امضای دیجیتال | محصول پشتیبانی |
| | <input type="checkbox"/> | ثبت‌نشان‌ها (داده‌های ممیزی) | می‌شوند، مشخص |
| | <input type="checkbox"/> | سایر موارد | گردد. |

| | | | |
|--------------------------------|-------------------------------------|--|---|
| | <input checked="" type="checkbox"/> | <p>۴ محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی^۴ معتبر را تولید یا از آن‌ها استفاده نماید.</p> | |
| | <input type="checkbox"/> | گرفتن مهرهای زمانی از سرور NTP | روش‌های ایجاد مهرهای زمانی معتبر |
| | <input type="checkbox"/> | تنظیم مهرهای زمانی از طریق اینترنت | انتخاب شود. (دیگر |
| | <input checked="" type="checkbox"/> | تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز) | روشهای موجود در محصول، در قسمت |
| | <input type="checkbox"/> | سایر موارد | «سایر موارد» بیان شود). |
| | <input checked="" type="checkbox"/> | <p>۵ محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.</p> | |
| | <input checked="" type="checkbox"/> | بروزرسانی دستی | روش بروزرسانی مورد استفاده در محصول، |
| | <input type="checkbox"/> | جستجوی خودکار بروزرسانی‌ها | مشخص گردد (حداقل |
| | <input type="checkbox"/> | بروزرسانی‌های خودکار | یک مورد لازم و کافی است). |
| | <input type="checkbox"/> | بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی | |
| | <input type="checkbox"/> | <p>۶ در صورت استفاده از بروزرسانی به روش خودکار، محصول باید پیش از نصب بروزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.</p> | |
| | <input type="checkbox"/> | امضای دیجیتال | سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) |
| طبق نیازمندیهای نرم افزار نیست | <input type="checkbox"/> | درهم‌ساز منتشرشده | به‌روزرسانی‌ها انتخاب گردد. |

^۴ Time stamp

۲-۷- تخصیص منابع

در این رده، به بررسی وضعیت عملکردهای محصول و منابع مورد استفاده توسط آن در زمانهای مختلف از جمله زمان شکست پرداخته می‌شود.

| توضیحات | رده تخصیص منابع | شماره الزام |
|---------|---|-------------|
| | <input checked="" type="checkbox"/> محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید. | ۱ |

۲-۸- دسترسی به محصول

در این رده توانایی محصول در مدیریت نشست‌های صورت گرفته شده توسط کاربر، ارزیابی می‌شود.

| توضیحات | رده دسترسی به محصول | | شماره الزام | | | | | | | |
|-------------------------------------|-------------------------------------|---|-------------------------------------|-----|---------------------------------|-------------------------------------|------|--------------------------|------------|---|
| | <input checked="" type="checkbox"/> | محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید. | ۱ | | | | | | | |
| | <input checked="" type="checkbox"/> | محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد. | ۲ | | | | | | | |
| | <input checked="" type="checkbox"/> | محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد. | ۳ | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.</p> <table border="1" data-bbox="919 943 1711 1097"> <tr> <td data-bbox="919 943 961 992" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="961 943 1711 992">روز</td> <td data-bbox="1711 943 1948 1097" rowspan="3">انتخاب یک مورد لازم و کافی است.</td> </tr> <tr> <td data-bbox="919 992 961 1040" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="961 992 1711 1040">زمان</td> </tr> <tr> <td data-bbox="919 1040 961 1097" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="961 1040 1711 1097">سایر موارد</td> </tr> </table> | <input checked="" type="checkbox"/> | روز | انتخاب یک مورد لازم و کافی است. | <input checked="" type="checkbox"/> | زمان | <input type="checkbox"/> | سایر موارد | ۴ |
| <input checked="" type="checkbox"/> | روز | انتخاب یک مورد لازم و کافی است. | | | | | | | | |
| <input checked="" type="checkbox"/> | زمان | | | | | | | | | |
| <input type="checkbox"/> | سایر موارد | | | | | | | | | |
| | <input checked="" type="checkbox"/> | <p>در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس موارد زیر و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.</p> <table border="1" data-bbox="919 1260 1711 1401"> <tr> <td data-bbox="919 1260 961 1308" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="961 1260 1711 1308">روز</td> <td data-bbox="1711 1260 1948 1401" rowspan="3">انتخاب یک مورد لازم و کافی است.</td> </tr> <tr> <td data-bbox="919 1308 961 1357" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="961 1308 1711 1357">زمان</td> </tr> <tr> <td data-bbox="919 1357 961 1401" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="961 1357 1711 1401">سایر موارد</td> </tr> </table> | <input checked="" type="checkbox"/> | روز | انتخاب یک مورد لازم و کافی است. | <input checked="" type="checkbox"/> | زمان | <input type="checkbox"/> | سایر موارد | ۵ |
| <input checked="" type="checkbox"/> | روز | انتخاب یک مورد لازم و کافی است. | | | | | | | | |
| <input checked="" type="checkbox"/> | زمان | | | | | | | | | |
| <input type="checkbox"/> | سایر موارد | | | | | | | | | |

| | | | |
|--|-------------------------------------|--|-----------------------|
| تنها مدیر سیستم یا کاربر مجاز دسترسی به این عملیات را دارد | <input checked="" type="checkbox"/> | محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید. | ۶ |
| | <input checked="" type="checkbox"/> | محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد. | ۷ |
| | <input checked="" type="checkbox"/> | مکان | پارامترهای موجود برای |
| | <input type="checkbox"/> | شماره پورت | جلوگیری از نشست، |
| | <input type="checkbox"/> | روز | مشخص شوند (وجود) |
| | <input type="checkbox"/> | زمان | یک مورد لازم و کافی |
| | <input checked="" type="checkbox"/> | سایر موارد | است). |

۲-۹- کانال‌ها/مسیرهای مورد اعتماد

در این رده به بررسی پروتکل‌های امنی که برای برقراری کانال/مسیر مورد اعتماد، بین محصول و موجودیت‌های IT خارجی، یا بین اجزای محصول، استفاده می‌شوند، پرداخته می‌شود.

| توضیحات | رده کانال‌ها/مسیرهای مورد اعتماد | | شماره الزام |
|---------|-------------------------------------|--|---|
| | <input checked="" type="checkbox"/> | محصول باید قادر باشد مسیر ارتباطی امنی بین خود، کاربران و دیگر محصولات IT فراهم نماید که به طور منطقی از دیگر کانال‌ها متمایز باشد. سپس از طریق این کانال احراز هویت را انجام دهد و از تغییر و افشای داده تبادل‌ی حفاظت نماید و تغییرات را تشخیص دهد. در صورت انتخاب مورد HTTPS، رعایت الزام ۱-۳- و ۳-۳- و در صورت انتخاب TLS، رعایت الزامات ۳-۲- تا ۳-۴- که در بخش ۳- بیان گردیده است، الزامی است. | ۱ |
| | <input type="checkbox"/> | HTTPS | پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد. |
| | <input checked="" type="checkbox"/> | TLS | |
| | <input type="checkbox"/> | SSH | |
| | <input checked="" type="checkbox"/> | محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند. | |
| | <input checked="" type="checkbox"/> | محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید. | |

۳- الزامات امنیتی مبتنی بر انتخاب

این بخش به بیان الزاماتی می‌پردازد که رعایت آنها وابسته به برخی از الزاماتی است که در بخش‌های پیشین بیان شده است. برای مثال اگر در الزامات مربوط به رده کانال امن، پروتکل HTTPS انتخاب شود، آنگاه رعایت الزامات HTTPS که در این بخش بیان شده است، اجباری می‌گردد.

۳-۱- پروتکل HTTPS

| شماره الزام | پروتکل HTTPS | توضیحات |
|-------------|--|-------------------------------------|
| ۱ | محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند. | <input checked="" type="checkbox"/> |
| ۲ | محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند. | <input checked="" type="checkbox"/> |
| ۳ | در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (در هنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید. اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش ۳-۵-۳ انجام می‌شود که در این صورت الزامات بخش ۳-۵-۳ الزامی است. | <input checked="" type="checkbox"/> |
| | محصول تنها از موارد اتصال را برقرار نکند. | <input checked="" type="checkbox"/> |
| | بیان شده می‌تواند استفاده نماید. برای برقراری اتصال درخواست مجوز کند. | <input type="checkbox"/> |

۲-۳- پروتکل TLS Client

| توضیحات | پروتکل TLS Client | | شماره الزام |
|--|---|---|-------------|
| <p>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 و TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</p> | <input checked="" type="checkbox"/> محصول باید TLS 1.2 (RFC 5246) و/یا TLS 1.1 (RFC 4346) را پیاده‌سازی و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید. | <p>مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.</p> | ۱ |
| | <input type="checkbox"/> TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 | | |
| | <input type="checkbox"/> TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 | | |
| | <input type="checkbox"/> TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 | | |
| | <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 | | |
| | <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 | | |
| | <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 | | |
| | <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 | | |
| | <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 | | |
| | <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 | | |
| <input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 | | | |

| | | | |
|-------------------------------------|--|--|--|
| <input type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 | | |
| <input type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 | | |
| <input type="checkbox"/> | TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 | | |
| <input type="checkbox"/> | TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246 | | |
| <input type="checkbox"/> | TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 | | |
| <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 | | |
| <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246 | | |
| <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 | | |
| <input checked="" type="checkbox"/> | TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 | | |
| <input type="checkbox"/> | TLS_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5288 | | |
| <input checked="" type="checkbox"/> | TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 | | |
| <input type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 | | |
| <input type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289 | | |
| <input type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289 | | |
| <input checked="" type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 | | |
| <input type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 | | |

| | | | |
|--|-------------------------------------|--|--|
| | | <input type="checkbox"/> مطابق با RFC 5289 <input checked="" type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 <input checked="" type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289 <input checked="" type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289 <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289 | |
| | <input checked="" type="checkbox"/> | محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125 تأیید نماید. | ۲ |
| | <input checked="" type="checkbox"/> | محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد؛ بنابراین اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید. | ۳ |
| | <input checked="" type="checkbox"/> | در صورت پشتیبانی از ارتباط را برقرار نکند | اقدامات دیگر، در «سایر موارد» بیان گردد. |
| | <input type="checkbox"/> | برای برقراری ارتباط درخواست مجوز کند | |
| | <input type="checkbox"/> | سایر موارد | |
| | <input checked="" type="checkbox"/> | محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید. | ۴ |
| | <input type="checkbox"/> | Supported Elliptic Curves Extension را ارائه نکند. | |

| | | | |
|--|--|---|--|
| | | <input checked="" type="checkbox"/> Supported Elliptic Curves Extension را به همراه NIST Curve های secp256r1 یا secp384r1 یا secp521r1 ارائه نماید. | در صورت که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد. |
|--|--|---|--|

۳-۳- پروتکل TLS Server

| توضیحات | پروتکل TLS Server | | شماره الزام | |
|---|-------------------------------------|--|--|--|
| <p>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</p> <p>TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256</p> | <input checked="" type="checkbox"/> | <p>محمول باید (RFC 5246) TLS 1.2 را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.</p> | <p>۱</p> <p>مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.</p> | |
| | | <p><input type="checkbox"/> TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268</p> | | |
| | | <p><input type="checkbox"/> TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268</p> | | |
| | | <p><input type="checkbox"/> TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268</p> | | |
| | | <p><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492</p> | | |
| | | <p><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492</p> | | |
| | | <p><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492</p> | | |
| | | <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492</p> | | |
| | | <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492</p> | | |
| | | <p><input type="checkbox"/> TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246</p> | | |
| | | <p><input type="checkbox"/> TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246</p> | | |
| | | <p><input type="checkbox"/> TLS_DHE_RSA_WITH_AES_128_CBC_SHA256</p> | | |

| | | | |
|--|-------------------------------------|--|---|
| | | <p>مطابق با RFC 5246</p> <p><input type="checkbox"/> TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246</p> <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289</p> <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289</p> <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289</p> <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289</p> <p><input checked="" type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289</p> <p><input checked="" type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289</p> | |
| | <input type="checkbox"/> | <p>محصول باید اتصال‌های کاربرانی که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و TLS1.1 دارند را رد نماید.</p> | ۲ |
| | <input checked="" type="checkbox"/> | <p>محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.</p> | ۳ |
| | <input checked="" type="checkbox"/> | <p>استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت</p> | <p>در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.</p> |
| | <input checked="" type="checkbox"/> | <p>پارامترهای ECDH با استفاده از NIST Curve های secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر</p> | |
| | <input checked="" type="checkbox"/> | <p>پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت</p> | |

۳-۴- پروتکل TLS مشترک کلاینت و سرور

لازم به ذکر است که الزاماتی که با عنوان پروتکل‌های TLS Server و TLS Client مطرح شده است، برای مباحث مرتبط به احراز هویت TLS Server و TLS Client نیز مطرح می‌گردد. در این بخش چند الزام که برای احراز هویت این پروتکل‌ها مطرح می‌گردد و برای هر دوی کلاینت و سرور نیز یکسان است و باید برای هر کدام مورد بررسی قرار گیرد، آورده شده است.

| توضیحات | پروتکل TLS مشترک کلاینت و سرور | | شماره الزام |
|---------|-------------------------------------|--|-------------|
| | <input checked="" type="checkbox"/> | محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید. | ۱ |
| | <input type="checkbox"/> | در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده کلاینت مورد انتظار بوده است، محصول نباید کانال امن را برقرار سازد. | ۲ |

۳-۵- اعتبارسنجی گواهی نامه

| توضیحات | اعتبارسنجی گواهی نامه | شماره الزام |
|---------|---|-----------------------------------|
| | <input checked="" type="checkbox"/> محصول باید گواهی نامه‌ها را بر اساس قوانین زیر تأیید کند. | ۱ |
| | <input checked="" type="checkbox"/> تأیید گواهی نامه RFC 5280 و تأیید مسیر گواهی نامه که از حداقل طول مسیر دو گواهی نامه پشتیبانی می‌کند. | |
| | <input checked="" type="checkbox"/> مسیر گواهی نامه باید با یک گواهی نامه CA امن پایان یابد. | |
| | <input checked="" type="checkbox"/> محصول باید برای تأیید مسیر یک گواهی نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی نامه‌های CA به حالت «TRUE» تنظیم شده است. | |
| | <input type="checkbox"/> پروتکل وضعیت گواهی نامه آنلاین (OCSP) مشخص شده در RFC 696 | |
| | <input type="checkbox"/> لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5280 بخش ۳، ۶ | روش‌های تأیید وضعیت |
| | <input type="checkbox"/> لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5759 بخش ۵ | فسخ گواهی نامه |
| | <input checked="" type="checkbox"/> هیچ روش فسخ دیگری | |
| | <input type="checkbox"/> گواهی نامه‌های مورد استفاده برای تأیید بروزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID) extendedKeyUsage خود داشته باشند. | قوانین تأیید بخش extendedKeyUsage |
| | <input type="checkbox"/> گواهی نامه‌های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند. | |

| | | |
|---|---|--|
| | <input type="checkbox"/> گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف « Client Authentication » (با id-kp1 یا OID 1.3.6.1.5.5.7.3.2) را در بخش extendedKeyUsage خود داشته باشند. | |
| | <input type="checkbox"/> گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید « OCSP Signing » (با id-pk9 یا OID 1.3.6.1.5.5.7.3.9) را در بخش extendedKeyUsage خود داشته باشند. | |
| ۲ | <input checked="" type="checkbox"/> محصول باید تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و همچنین، پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA بپذیرد. | |
| ۳ | <input checked="" type="checkbox"/> محصول باید برای پشتیبانی از احراز هویت برای موارد زیر، از گواهی‌نامه‌های X509v3 تعریف شده در RFC 5280 استفاده کند. | |
| | <input type="checkbox"/> HTTPS | در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد. |
| | <input checked="" type="checkbox"/> TLS | |
| | <input type="checkbox"/> SSH | |
| | <input type="checkbox"/> امضای کد برای بروزرسانی‌های نرم‌افزار سیستم | |
| | <input type="checkbox"/> امضای کد برای تأیید یکپارچگی | |
| | <input type="checkbox"/> سایر موارد | |
| | <input type="checkbox"/> | |

۳-۶- پروتکل SSH

| توضیحات | پروتکل SSH | شماره الزام |
|---------|--|-------------|
| | <input type="checkbox"/> محصول باید پروتکل SSH را مطابق با RFC های ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید. | ۱ |
| | <input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4252، از روش‌های احراز هویت زیر پشتیبانی نماید. | ۲ |
| | <input type="checkbox"/> احراز هویت مبتنی بر کلید عمومی | |
| | <input type="checkbox"/> احراز هویت مبتنی بر گذرواژه | |
| | <input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4253، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد. | ۳ |
| | <input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید. | ۴ |
| | <input type="checkbox"/> AES128-CBC | |
| | <input type="checkbox"/> AES192-CBC | |
| | <input type="checkbox"/> AES256-CBC | |
| | <input type="checkbox"/> AES128-CTR | |
| | <input type="checkbox"/> AES192-CTR | |
| | <input type="checkbox"/> AES256-CTR | |
| | <input type="checkbox"/> AEAD_AES_128_GCM | |
| | <input type="checkbox"/> AEAD_AES_256_GCM | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------|---|--------------------------|-------------------|--------------------------|------------------|--------------------------|---------------|--------------------------|---------------|--------------------------|---------------------|--------------------------|---------------------|--------------------------|---------------------|--------------------------|----------------------------|--------------------------|----------------------------|--------------------------|----------------------------|--------------------------|-----------------------|--------------------------|---------|--------------------------|----------------|---|
| | <p><input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های کلید عمومی زیر استفاده نماید.</p> <table border="1" data-bbox="919 266 1709 867"> <tr><td><input type="checkbox"/></td><td>ssh-ed25519</td></tr> <tr><td><input type="checkbox"/></td><td>ssh-ed448</td></tr> <tr><td><input type="checkbox"/></td><td>rsa-sha2-512</td></tr> <tr><td><input type="checkbox"/></td><td>rsa-sha2-256</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp521</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp384</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp256</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp521</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp384</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp256</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-rsa2048-sha256</td></tr> <tr><td><input type="checkbox"/></td><td>ssh-rsa</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ssh-rsa</td></tr> </table> | <input type="checkbox"/> | ssh-ed25519 | <input type="checkbox"/> | ssh-ed448 | <input type="checkbox"/> | rsa-sha2-512 | <input type="checkbox"/> | rsa-sha2-256 | <input type="checkbox"/> | ecdsa-sha2-nistp521 | <input type="checkbox"/> | ecdsa-sha2-nistp384 | <input type="checkbox"/> | ecdsa-sha2-nistp256 | <input type="checkbox"/> | x509v3-ecdsa-sha2-nistp521 | <input type="checkbox"/> | x509v3-ecdsa-sha2-nistp384 | <input type="checkbox"/> | x509v3-ecdsa-sha2-nistp256 | <input type="checkbox"/> | x509v3-rsa2048-sha256 | <input type="checkbox"/> | ssh-rsa | <input type="checkbox"/> | x509v3-ssh-rsa | ۵ |
| <input type="checkbox"/> | ssh-ed25519 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | ssh-ed448 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | rsa-sha2-512 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | rsa-sha2-256 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | ecdsa-sha2-nistp521 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | ecdsa-sha2-nistp384 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | ecdsa-sha2-nistp256 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | x509v3-ecdsa-sha2-nistp521 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | x509v3-ecdsa-sha2-nistp384 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | x509v3-ecdsa-sha2-nistp256 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | x509v3-rsa2048-sha256 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | ssh-rsa | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | x509v3-ssh-rsa | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <p><input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های MAC صحت داده‌های زیر استفاده نماید.</p> <table border="1" data-bbox="919 980 1709 1260"> <tr><td><input type="checkbox"/></td><td>AEAD_AES_256_GCM</td></tr> <tr><td><input type="checkbox"/></td><td>AEAD_AES_128_GCM</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha2-512</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha2-256</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha1-96</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha1</td></tr> </table> | <input type="checkbox"/> | AEAD_AES_256_GCM | <input type="checkbox"/> | AEAD_AES_128_GCM | <input type="checkbox"/> | hmac-sha2-512 | <input type="checkbox"/> | hmac-sha2-256 | <input type="checkbox"/> | hmac-sha1-96 | <input type="checkbox"/> | hmac-sha1 | ۶ | | | | | | | | | | | | | | |
| <input type="checkbox"/> | AEAD_AES_256_GCM | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | AEAD_AES_128_GCM | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | hmac-sha2-512 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | hmac-sha2-256 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | hmac-sha1-96 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | hmac-sha1 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <p><input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.</p> <table border="1" data-bbox="919 1373 1709 1463"> <tr><td><input type="checkbox"/></td><td>curve25519-sha256</td></tr> <tr><td><input type="checkbox"/></td><td>curve448-sha512</td></tr> </table> | <input type="checkbox"/> | curve25519-sha256 | <input type="checkbox"/> | curve448-sha512 | ۷ | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | curve25519-sha256 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | curve448-sha512 | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | |
|--|--------------------------|---|---|
| | <input type="checkbox"/> | diffie-hellman-group-exchange-sha256 diffie-hellman-group18-sha512 diffie-hellman-group17-sha512 diffie-hellman-group16-sha512 diffie-hellman-group15-sha512 ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 rsa2048-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 | |
| | <input type="checkbox"/> | محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه (طول نشست بیشتر از یک ساعت و حجم داده مبادله شده بیشتر از ۱ گیگابایت نباشد) استفاده گردد. در صورت پر شدن حد آستانه برای هر کدام از موارد ذکر شده، باید تجدید کلید صورت بگیرد. | ۸ |
| | <input type="checkbox"/> | محصول باید اطمینان حاصل نماید که کلاینت SSH، سرور SSH را احراز هویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن (تشریح شده در RFC 4251 بخش ۱.۷) همراه می‌کند، استفاده می‌نماید. | ۹ |