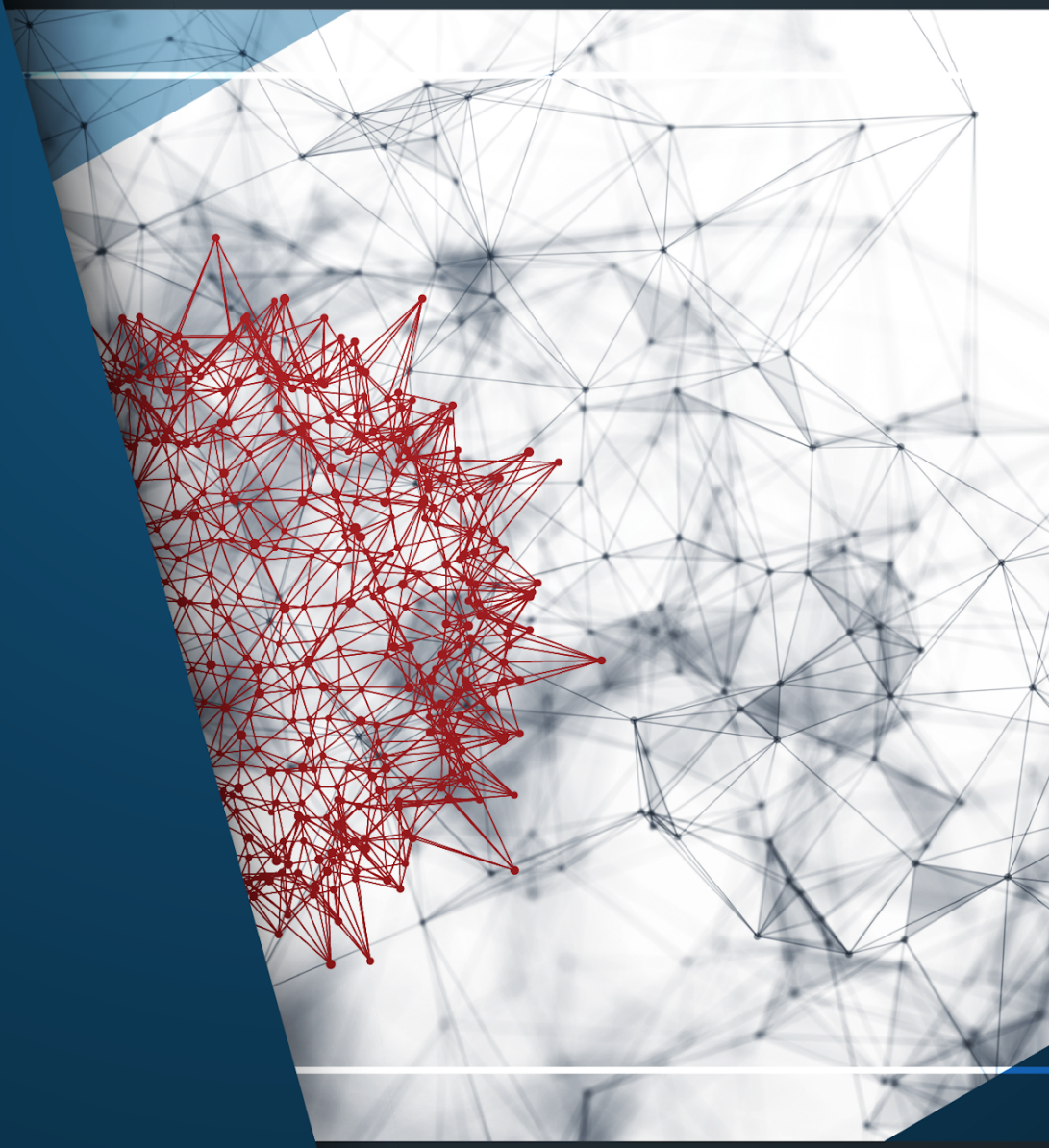
amatas

РЕЗЮМЕ НА ДОКЛАД ЗА ОДИТ НА ИНФОРМАЦИОННАТА СИГУРНОСТ НА ЦССРД



2020

www.amatas.com

РЕЗЮМЕ НА ДОКЛАД ЗА ОДИТ НА ИНФОРМАЦИОННАТА СИГУРНОСТ НА ЦЕНТРАЛИЗИРАНАТА СИСТЕМА ЗА СЛУЧАЙНО РАЗПРЕДЕЛЕНИЕ НА ДЕЛАТА

В изпълнение на сключен договор с Висшия съдебен съвет, през периода 17 февруари 2020 г. – 9 март 2020 г. от страна на „АМАТАС“ ЕАД е извършен одит на информационната сигурност на Централизираната система за случайно разпределение на делата (ЦССРД), с оглед ограничаване на вътрешни и външни уязвимости. Одитът е извършен с цел установяване на налични уязвимости на системата, като е симулирана дейност от злонамерен нападател, за да се установи до какви ресурси от тествaната система такъв нападател би могъл да осъществи достъп, както и какви промени може да нанесе по системата. С цел да се предотвратят проблеми по отношение на нормалното функциониране на системата, за целите на одита продукционната среда е репликирана в тестова такава.

Централизираната система за случайно разпределение на делата физически е разположена на сървър на Висшия съдебен съвет. Достъпът до нея е ограничен до конкретни ползватели и други технически лица, отговарящи за нейната техническа поддръжка и се осигурява посредством три слоя на защита.

При одита е направен анализ на конфигурацията на сървъра, на който е разположена ЦССРД, на базата данни, на кода на приложението и на журналните записи за използване на системата. За тестването са използвани автоматизирани и полуавтоматизирани софтуерни решения, извършени са оценки и проверки от страна на експерти по киберсигурност.
Одитните действия са извършени по начин, който да осигури опазването на нормалната функционалност на системата.

При одита са установени общо 23 технически уязвимости, нивото на риск на които е изчислено спрямо Common Vulnerability Scoring System (https://www.first.org/cvss/). Установените уязвимости са, както следва:

I. С високо ниво на риск – 11 (47,8%) – уязвимости, свързани с достъпа до системата, както и такива, които в рамките на ЦССРД предоставят възможност за нарушаване на сигурността на системата чрез:
- неоторизирано добавяне на нов съд;

- неоторизирана редакция на чужд съд;
- неоторизирана редакция на съдии от друг съд;
- неоторизирана редакция на групи от съдии от чужд съд;
- неоторизирано изтриване на инкрементални номера;
- неоторизирано изтриване на отсъствия;
- неоторизирано изтриване на регистрирани дежурства;
- неоторизиран достъп до данни на потребители от чужд съд;
- неоторизирано разпределение на дело на съдия от чужд съд.

II. Със средно ниво на риск – 2 (8,7%) – уязвимости, които в рамките на системата осигуряват потенциална възможност за нарушаване поверителността на информацията в ЦССРД чрез:

- разкриване на информация за съществуващи потребители;
- разкриване на информация за съществуващи съдии.

III. С ниско ниво на риск – 10 (43,5%) – уязвимости, свързани с настройките за сигурност на системни елементи – част от ЦССРД и предварително изискващи достъп до сървъра:

- уязвимост тип „Hotlinking“;
- недостатъчна продължителност на заключване на акаунт (Local Group Policy);
- възможност за добавяне на компютър / устройство към домейн контролер (Local Group Policy);
- възможност за генериране на системни доклади от операционната система (Local Group Policy);
- възможност за вписване като „batch job“ (Local Group Policy);
- възможност за заместване на токен на процес (Local Group Policy);
- възможност за спиране на операционната система (Local Group Policy);
- възможност за блокиране на Microsoft акаунти (Local Group Policy);
- възможност за преименуване на посетителски акаунти (Local Group Policy);
- възможност за форматиране на закачени преносими устройства (Local Group Policy).

Установените при одита уязвимости представляват риск, като експлоатирането на част от тях би могло, при наличието на допълнителни предпоставки, в това число и

предварително осигурен достъп, да доведе до неоторизирани промени в резултатите от разпределението на дела.

Тестовете за оценка на сигурността не са установили техническа възможност за достъп до системата отдалечено, без съответното лице да бъде предварително и ръчно оторизирано от лицата, отговорни за това.

В рамките на договорно определения обхват, одитиращото дружество не е имало задача да извършва проверки за установяване на действителни нарушения на сигурността на системата, в т.ч. за осъществен неоторизиран достъп и за извършени манипулации при разпределението на дела от ЦССРД, и такива проверки не са извършвани. Въпреки това, по време на тестовете за оценка на сигурността са забелязани журнални файлове със следи от потенциално злонамерена дейност спрямо системата на ЦССРД от страна на IP адрес с локация гр. София. Опитите за неоторизиран достъп до базата данни са се състояли между 22:38 ч. и 22:47 ч. на 4-ти октомври 2016 година, като за същите са използвани автоматизирани инструменти. Няма информация относно получения отговор от страна на сървъра.

На база резултатите от одита е констатирано, че ЦССРД е разработена с фокус върху нейната функционалност. В същото време, системата не е защитена с достатъчно надеждни контроли за сигурност от техническа гледна точка, съответстващи на нейното предназначение и отговарящи на добрите практики и стандарти по информационна сигурност, тъй като системата използва остарели технологии.

Въз основа на констатираните уязвимости, с одитния доклад са дадени конкретни препоръки за тяхното отстраняване, както и за цялостното подобряване на сигурността на ЦССРД. Специални препоръки са дадени по отношение на уязвимостите, свързани с достъпването на системата, доколкото такива уязвимости са една от най-често срещаните причини за компрометиране на информационни системи и същите могат да позволят на външни лица да достъпят директно базите данни и по този начин да извършат нерегламентирани дейности, с които да нарушат интрегритета на тези данни.

Изготвил:

Екип на „АМАТАС“ ЕАД