ASTRA LINUX®

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СРЕДСТВ ЗАЩИТЫ **ASTRA LINUX SPECIAL EDITION** ПРИ ВЫЯВЛЕНИИ УЯЗВИМОСТЕЙ НУЛЕВОГО ДНЯ

Мылицын Роман
Astra Linux

ЗАЩИТА ВАШИХ ДАННЫХ

ASTRA LINUX®

Комплекс различных средств информации, встроенных в операционную систему, опирающийся на математическую модель

- ПЕРСОНАЛЬНЫЕ ДАННЫЕ
- КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ
- КОММЕРЧЕСКАЯ ТАЙНА
- СЕКРЕТНЫЕ
- СОВЕРШЕННО СЕКРЕТНЫЕ
- ОСОБОЙ ВАЖНОСТИ

> 5 000
СЕРТИФИЦИРОВАННЫХ ПРИЛОЖЕНИЙ В ПАКЕТНОМ РЕПОЗИТОРИИ

~25 000
ПРОГРАММ В РОССИЙСКОМ РЕПОЗИТОРИИ ASTRA LINUX

- Электронная почта
- Управление единым пространством пользователя
- Средства резервного копирования
- Мультимедиа
- Интернет-браузер
- Web-серверы
- Офисные приложения
- Средства документооборота
- СУБД

УРОВНИ ЦЕЛОСТНОСТИ

ASTRA LINUX®

Mandatory integrity control
Обязательный контроль целостности
Контроль учетных записей (UAC)
Мандатный контроль целостности

МОНИТОР ОБРАЩЕНИЙ

ТОКЕН, МАРКЕР, МЕТКА

УРОВНИ ЦЕЛОСТНОСТИ

Windows

- Недоверенный 0
- Низкий 100
- Средний 200
- Высокий 300
- Системный 400

Astra Linux

- 0 Нулевой уровень
- 1 Сетевые службы
- 2 Виртуализация
- 4 Специальное ПО
- 8 Графический сервер
- 16 СУБД

ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА

ASTRA LINUX®

- Внедрение подписи в исполняемые файлы и в расширенные атрибуты файловой системы
- Блокирование запуска недоверенного ПО
- Защита от подмены приложений

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

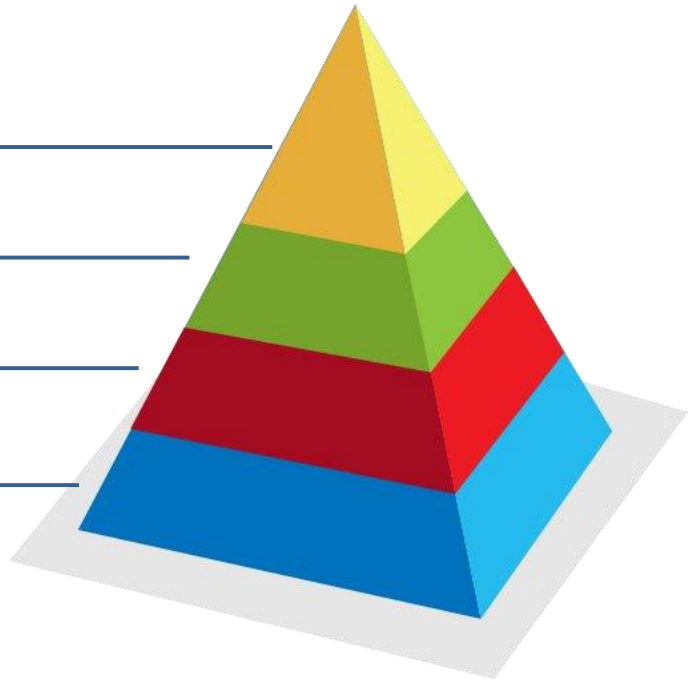
ASTRA LINUX®

Приложения

Замкнутая программная среда

Мандатный контроль целостности

Astra Linux Special Edition



КАК ЭТО РАБОТАЕТ НА ПРАКТИКЕ

ASTRA LINUX®

Коммерсантъ

$ 77,07 € 87,09 IMOEX 3432,11 Олимпиада в Пекине Обострение вокруг Украины Валютный прогноз

Информационная безопасность

27.01.2022, 01:05

Linux нараспашку

В системе найдена врожденная уязвимость

11K 20 3 мин.

Qualys обнаружила уязвимость в открытой операционной системе (ОС) Linux, которая существует с момента появления ОС и может наделить правами администратора любого пользователя. Под угрозой оказались и российские операционные системы на базе Linux, которые установлены в банках, на промышленных объектах и в госсекторе. Разработчики отечественных ОС на Linux уже начали публиковать обновления, закрывающие пробел в безопасности. Но проблема может быть не единичной, поскольку комплексно исследованием исходного кода Linux мало кто занимался, считают эксперты.

АТАКИ НУЛЕВОГО ДНЯ

ASTRA LINUX®

- Уязвимы практически все дистрибутивы Linux
- Крайняя простота эксплуатации
- Уязвимость существовала много лет
- **КАК ПРОТИВОСТОЯТЬ ТАКИМ АТАКАМ?**

ПРОТИВОДЕЙСТВИЕ ЭКСПЛУАТАЦИИ УЯЗВИМОСТИ

ASTRA LINUX®

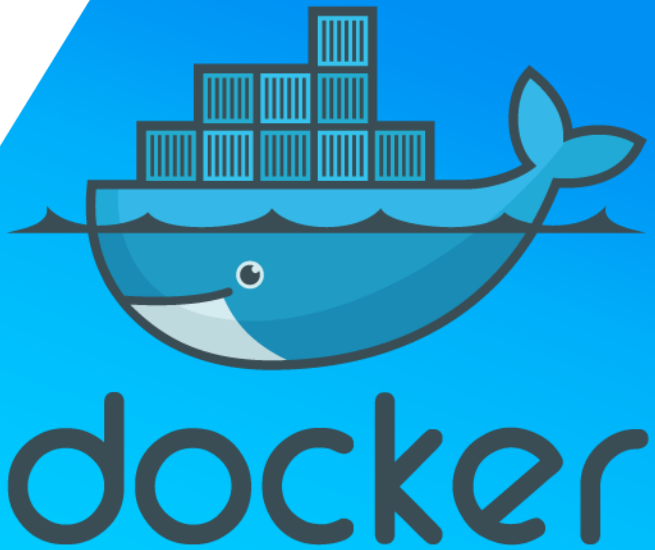
ASTRA LINUX SPECIAL EDITION

- На первом этапе загрузку «полезной нагрузки» эксплоита блокирует механизм замкнутой программной среды (ЗПС)
- Если удалось обойти ЗПС, процесс, получивший права root (id=0), не получает метку высокой целостности
- Монитор обращений блокирует все попытки процесса без метки повлиять на системные файлы или процессы
- Итог: злоумышленник не может получить контроль над системой

ДАЛЬНЕЙШЕЕ РАЗВИТИЕ МЕХАНИЗМОВ МКЦ

ASTRA LINUX®

- Запуск контейнеров на изолированном уровне целостности
- Возможность реализации песочниц для недоверенного ПО
- Изолированные и частично изолированные уровни целостности (доверия)



ВОПРОСЫ?

ASTRA LINUX®

Терминал Fly

Файл Правка Настройка Справка

ls

```
root@astra:/home/user# pdp-id
Уровень конф.=0(Уровень_0), Уровень целостности:0(Низкий), Категории=
Роли=:(Нет:Нет)
root@astra:/home/user# modprobe parport_pc
modprobe: ERROR: could not insert 'parport_pc': Permission denied
root@astra:/home/user#
root@astra:/home/user#
root@astra:/home/user# pdp-ls -M /dev/sda
brw-rw----m--  1 root disk Уровень_3:Высокий:Категория_1,Категория_2,
root@astra:/home/user#
root@astra:/home/user# dd if=/dev/sda of=~/sda.img count=3
dd: не удалось открыть '/dev/sda': Операция не позволена
root@astra:/home/user#
```

СПАСИБО ЗА ВНИМАНИЕ!

ЛЕГКОГО ИМПОРТОЗАМЕЩЕНИЯ С ASTRA LINUX