KASPERSKY lab

Защищенное сетевое оборудование от «Лаборатории Касперского» и «ЭЛТЕКС»

Kaspersky® Security System

www.kaspersky.ru
os.kaspersky.ru

ELTEX

eltex-co.ru

Две ведущие российские компании объединили усилия для создания защищенного телекоммуникационного оборудования

«Целевые атаки на корпоративные и индустриальные сети нередко осуществляются через уязвимости в базовом программном обеспечении, но в то же время именно оно на сегодняшний день защищено недостаточно надежно».

Андрей Духвалов, руководитель управления перспективных технологий «Лаборатории Касперского»

«Объем и уровень информационных угроз растут с каждым годом. Как производителю и разработчику устройств, нам необходимо использовать самые современные технологии защиты оборудования, чтобы обеспечить его безопасную и надежную работу в сетях наших заказчиков. Использование решения KSS от «Лаборатории Касперского» позволило нам добиться нового уровня безопасности устройств производства ЭЛТЕКС».

Михаил Моисеев, заместитель коммерческого директора «ЭЛТЕКС»

Задача

Современные системы телекоммуникаций обладают широким функционалом, но с ростом возможностей увеличивается и количество киберугроз, подвергающих риску как стабильность работы самого оборудования, так и безопасность и конфиденциальность передаваемых и хранимых данных.

Поэтому современное телекоммуникационное оборудование, помимо выполнения своих основных функций, должно обеспечивать кибербезопасность самого устройства и передаваемых через него данных. При этом конечные пользователи должны быть уверены в том, что устройство не содержит недокументированного функционала. Учитывая все вышеизложенное, представляется необходимым создание базового программного обеспечения со встроенной защитой от киберугроз и его установка на доверенное оборудование.

Решение

Компании «ЭЛТЕКС» и «Лаборатория Касперского» объединили свои усилия для создания доверенного телекоммуникационного решения, максимально удовлетворяющего требованиям кибербезопасности. За основу были взяты программно-аппаратные продукты компании «ЭЛТЕКС» и модуль безопасности Kaspersky Security System (KSS). При этом все настройки безопасности, в том числе запреты на выполнение определенных процессов и действий, учитывают особенности оборудования компании «ЭЛТЕКС» и требования к его безопасности. Таким образом, аппаратно-программное средство «ЭЛТЕКС» само надежно защищено от возможных кибератак.

Интеграция KSS в решение «ЭЛТЕКС» была осуществлена одновременно с изменением архитектуры. С точки зрения архитектуры, в решении можно выделить несколько основных компонентов:

- **CLI Shell:** command line interface shell, интерфейс командной строки, который используется пользователями системы для задач конфигурирования устройства, запуска вспомогательных утилит, анализа логов и т.д.;

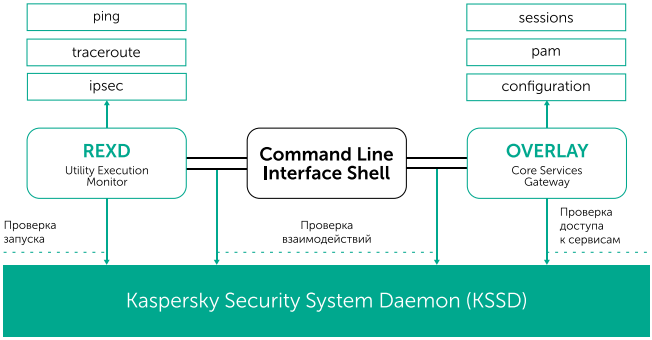
Kaspersky Security System контролирует взаимодействие программных компонентов внутри информационной системы на основе предварительно описанных свойств безопасности и правил этого взаимодействия, а также фиксирует и блокирует отклонения, вызванные внутренними ошибками или попытками несанкционированного доступа.

CLI Shell - это сложный компонент, непосредственно взаимодействующий с удаленным пользователем.

Основные особенности KSS/ Linux:

- изоляция отдельных компонентов решения с использованием технологии контейнеризации
- формальное описание интерфейсов всех компонентов и валидация передаваемых сообщений на соответствие этим интерфейсам
- средство контроля всех межкомпонентных взаимодействий на соответствие специфицированной политике безопасности
- инструменты для спецификации политики безопасности в виде комбинации широкого набора свойств безопасности, задаваемых в декларативном стиле в терминах предметной области

- **OVERLAY:** основные сервисы устройства, такие как аутентификация, конфигурирование, журналирование и т.д.;
- **REXD:** сервис запуска вспомогательных команд, к нему CLI Shell обращается для запуска большого числа утилит, таких как ping, traceroute, tcpdump и многих других;
- **KSSD:** сервис обмена сообщениями и проверки доступа в соответствии с политикой безопасности.



Основная цель интеграции KSS - исключить несанкционированное повышение пользователем своих привилегий, даже в условиях полной компрометации CLI Shell. Другими словами, CLI Shell рассматривается как недоверенный компонент.

Для каждого вновь подключенного пользователя стартует новый экземпляр CLI Shell, которому присваивается определенный уровень привилегий (от 0 до 15). В процессе работы, пользователь может повысить свои привилегии с помощью команды enable, требующей дополнительной авторизации. KSSD знает в каждый момент времени знает полученный через авторизацию уровень привилегий для всех экземпляров CLI Shell.

В соответствии с ограничениями, накладываемыми политикой безопасности, с каждой командой связан минимальный уровень привилегий, необходимый для ее запуска. При каждом запросе со стороны CLI Shell, KSSD производит проверку, достаточен ли текущий уровень привилегий для данной команды.

Результат

Примененный комплекс мер позволяет утверждать, что пользователь с уровнем привилегий менее 10 не сможет выполнить ни одной привилегированной команды, даже в случае обнаружения и эксплуатации критической уязвимости в CLI Shell. Таким образом, благодаря тесному сотрудничеству двух отраслевых лидеров был создан новый продукт. Пользователи нового решения, которое уже поступило в продажу, могут быть уверены, что их оборудование неуязвимо для атак, а данные надежно защищены.

О «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и двадцатилетний опыт борьбы с киберугрозами лежат в основе защитных решений и сервисов компании, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и более 270 тысяч корпоративных клиентов по всему миру.

О компании «ЭЛТЕКС»

ООО «Предприятие «ЭЛТЕКС» – ведущий российский разработчик и производитель сетевого и телекоммуникационного оборудования.

Предприятие основано в 1992 году и на сегодняшний день является крупной, динамично развивающейся компанией. Численность сотрудников составляет более 600 человек.

«ЭЛТЕКС» имеет собственное высокотехнологичное производство, включающее все необходимые технологические циклы и оборудование, а также 7 лабораторий по разработке ПО.

На изображении представлены сервисные маршрутизаторы моделей ESR-1200, ESR-1000 и ESR-12VF.
С полным списком защищенного оборудования можно ознакомиться на сайте «ЭЛТЕКС»:
https://eltex-co.ru/catalog/service_gateways/

KasperskyOS®

Подробнее на:
os.kaspersky.ru

www.kaspersky.ru