Безопасность тонких клиентов

Уязвимости тонких клиентов

Тонкий клиент состоит из множества компонентов, работающих под управлением операционной системы. К сожалению, программный код не идеален и содержит ошибки, которые приводят к уязвимостям. Уязвимости могут быть использованы злоумышленниками для обхода механизмов защиты и компрометации устройства и, в конечном счёте, нанесению ущерба компании.

Известные уязвимости:

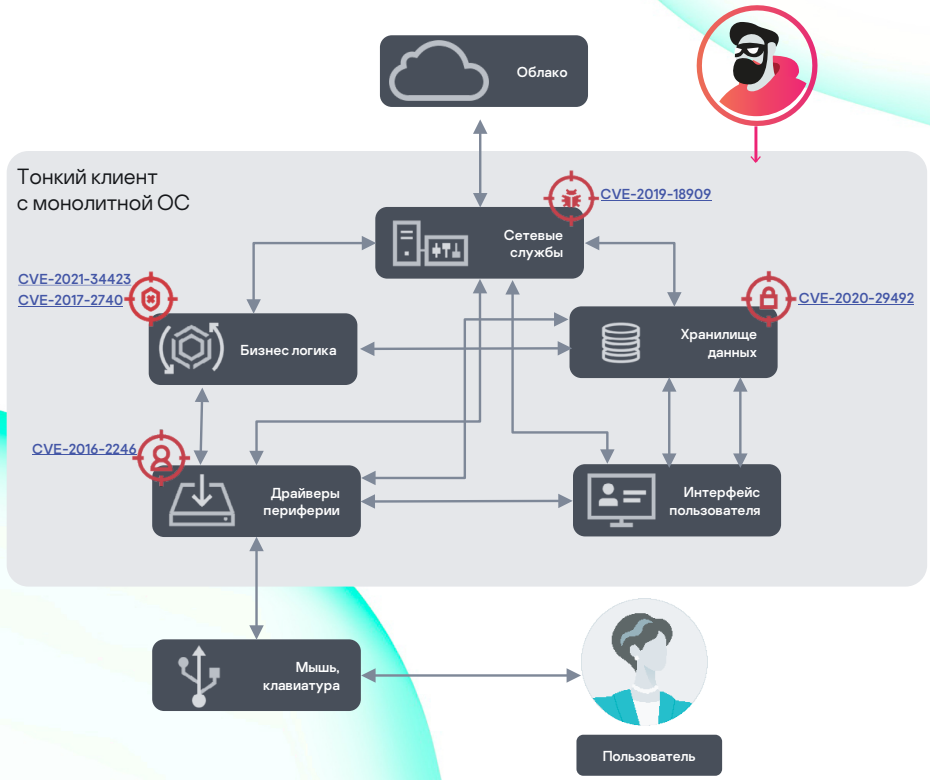
CVE-2021-34423
Благодаря arbitrary code execution, можно продвигаться дальше по системе, пользуясь уязвимостью монолитной ОС.

CVE-2017-2740
Повышение привилегий через command line shell.

CVE-2016-2246
Повышение привилегий. Эксплуатация происходит через виртуальную клавиатуру, запущенную от root.

CVE-2020-29492
FTP-сервер, используемый для обновления прошивки устройств, позволяет пользователю anonymous отредактировать ini-файл, используемый для конфигурации – by design. Что приводит к исполнению произвольного кода тонком клиенте и на машине, к которой устройство подключается.

CVE-2019-18909
Через уязвимость в плагине возможно получить исполнение произвольного кода с правами root.



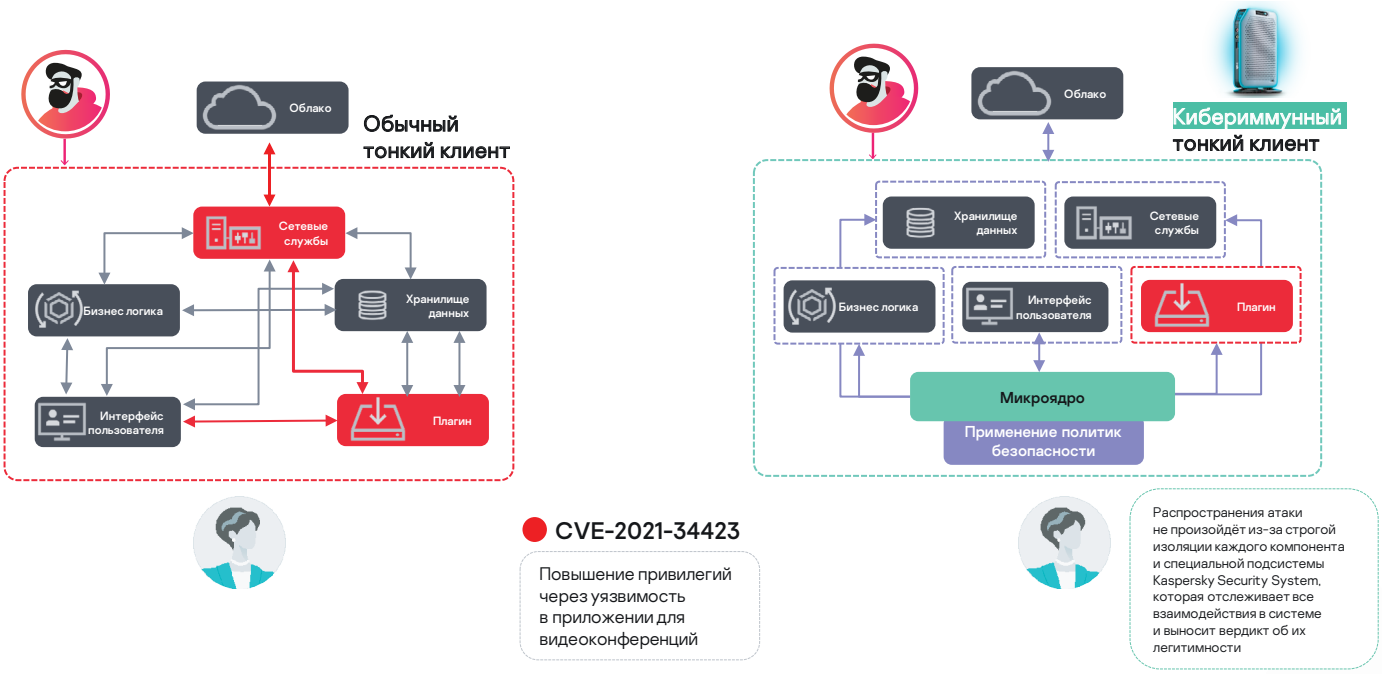
Сценарий развития кибератаки на обычный тонкий клиент и кибериммунный

Рассмотрим случай, когда пользователь тонкого клиента получает от злоумышленника фишинговое письмо для подключения к веб-конференции в одном из популярных сервисов для видеоконференции. Сама по себе ссылка не несёт вреда и является вполне легитимной, однако подключившись к конференции, пользователь получает особым образом составленное сообщение в чат, что приводит к эксплуатации уязвимости CVE-2021-34423.

Так как большинство тонких клиентов работает под управлением операционной системы с монолитным ядром, то в результате из-за ошибки переполнения буфера внутри плагина приложения, злоумышленник может получить права администратора во всей системе.

В дальнейшем злоумышленник может развить атаку, установив шпионское ПО и похитив данные учётной записи пользователя. Если работа сотрудника связана с доступом к критическим сервисам компании, к примеру казначейству, то злоумышленник может нанести прямой финансовый урон, сформировав платёжное поручение по заведомо подложным реквизитам.

KasperskyOS



Сценарии атаки на обычный и киберимунный тонкие клиенты

Кибериммунитет — это «врожденная» защищенность IT-системы, ее способность противостоять кибератакам без использования дополнительных наложенных средств безопасности. Подавляющее большинство видов атак на кибериммунную систему неэффективно и не может повлиять на выполнение ею критических функций. Кибериммунные продукты практически невозможно скомпрометировать в плановых режимах работы, в них принципиально минимизировано число возможных уязвимостей.

В случае с кибериммунным тонким клиентом эта атака не приведёт к столь тяжким последствиям. Используя уязвимость CVE-2021-34423 или любую другую, в том числе уязвимость нулевого дня, атаке подвергнется лишь небольшая, изолированная область памяти, отведённая под работу плагина. Распространения атаки не произойдёт не только из-за строгой изоляции, которую обеспечивает микроядро KasperskyOS, но и из-за специальной подсистемы Kaspersky Security System, которая отслеживает все взаимодействия в системе и выносит вердикт об их легитимности.

Кибериммунные продукты являются следующим шагом обеспечения безопасности из-за самого подхода к защите. Наряду с общепринятыми практиками безопасной разработки, кибериммунные продукты создаются по принципу Secure by Design, т.е. чтобы быть изначально безопасными в условиях агрессивной среды, а не полагаться на средства наложенной защиты.

Kaspersky Secure Remote Workspace – решение для построения управляемой и функциональной инфраструктуры тонких клиентов на базе кибериммунной операционной системы KasperskyOS для защищенного подключения к VDI.

Дополнительная информация

Узнайте больше о возможностях Kaspersky Secure Remote Workspace и отправьте заявку на консультацию экспертов: os.kaspersky.ru/solutions/kaspersky-secure-remote-workspace

os.kaspersky.ru
www.kaspersky.ru

KasperskyOS