



Сделать вселенную безопаснее:

**Positive Technologies
выявляет уязвимости**

«В программах встречаются ошибки. Это нормально», — писал Давид Хейнемейер Ханссон, разработчик фреймворка Ruby on Rails. Но если эти ошибки не исправлять, то это может привести к серьезным финансовым последствиям и даже человеческим жертвам. Например, недостатки в системе обработки багажа в аэропорту «Хитроу» привели к потере 42 000 чемоданов и отмене 500 авиарейсов в течение первых 10 дней после открытия нового терминала. Недостаточно протестированное ПО для высокочастотной торговли за полчаса спустило на бирже 440 млн \$ — почти весь капитал американского брокера Knight Capital Group. И таких примеров множество.

Поиск и устранение уязвимостей — это совместная работа разработчиков ПО и экспертов по ИБ. Positive Technologies принимает активное участие в этом процессе и регулярно предоставляет производителям ПО сведения о новых уязвимостях. Наша компания руководствуется принципами ответственного разглашения (responsible disclosure). Это значит, что всю имеющуюся у нас информацию о выявленных уязвимостях мы в первую очередь предоставляем производителю данного ПО, включая подробности эксплуатации и рекомендации по защите. Лишь после устранения недостатков и выпуска официальных обновлений безопасности, по договоренности с вендором, мы публикуем результаты наших исследований в интернете. Работа по выявлению уязвимостей направлена на повышение уровня защищенности от киберугроз по всему миру. Ведь если эксперты перестанут указывать производителям на их ошибки и помогать с исправлениями, то преступники обнаружат уязвимости первыми и воспользуются ими без предупреждений. А это неприемлемо.

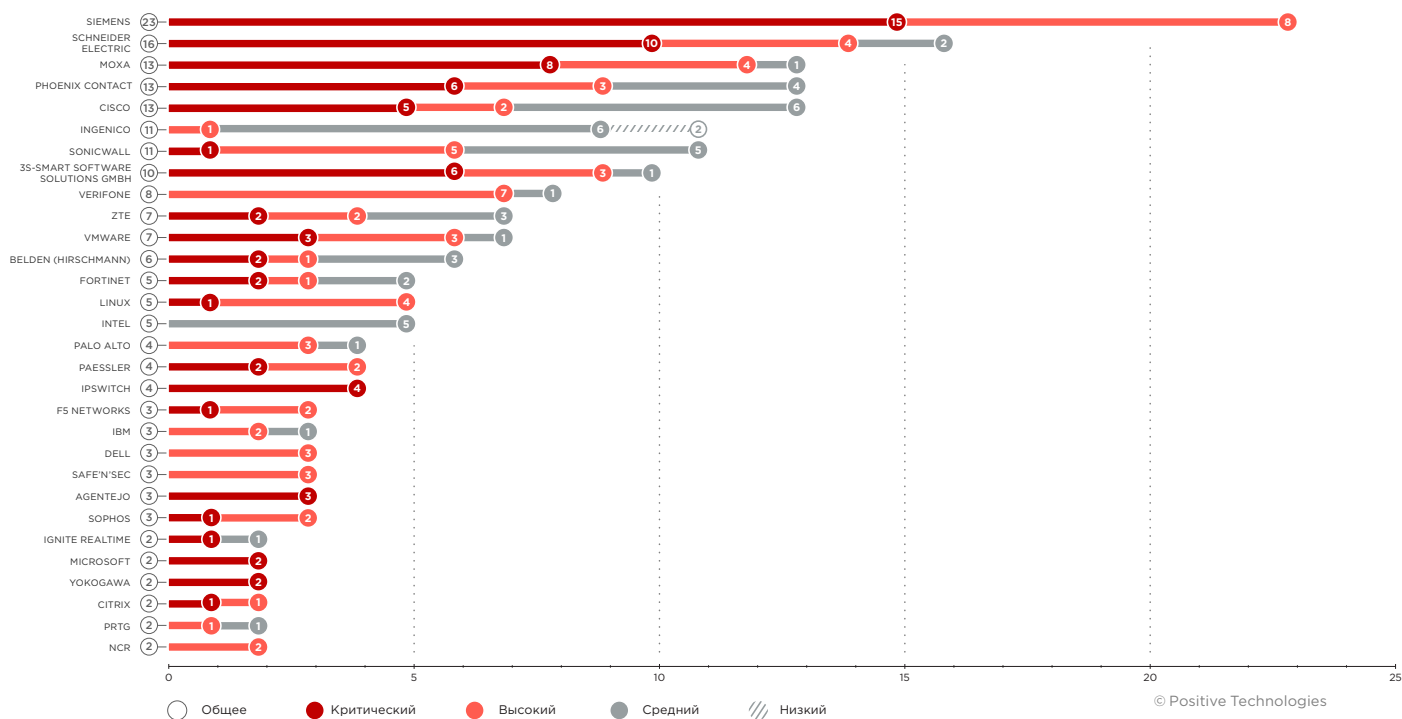
Основной сценарий взаимодействия с производителем после обнаружения уязвимости экспертами Positive Technologies



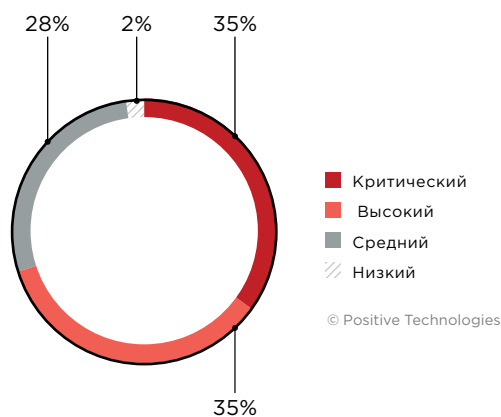
Результаты трехлетней работы

За период с 2018 по 2021 год эксперты Positive Technologies выявили более 250 уязвимостей в программных продуктах 60 различных производителей, среди которых [Cisco](#), [Citrix](#), [IBM](#), [Ingenico](#), [Intel](#), [Fortinet](#), [Palo Alto](#), [Microsoft](#), [VMware](#), [Hirschmann](#), [Moxa](#), [NCR](#), [Schneider Electric](#), [Siemens](#), [Verifone](#), [Yokogawa](#). В настоящий момент 27 уязвимостей ожидают подтверждения от вендоров.

Наибольшее количество опасных уязвимостей за последние три года было выявлено в программных и аппаратных продуктах следующих производителей.



Топ-30 вендоров по количеству и уровню опасности уязвимостей, выявленных за последние три года экспертами Positive Technologies



Уровень опасности выявленных уязвимостей

70% выявленных уязвимостей имели высокий или критический уровень риска согласно системе оценок CVSS 3.0. Уязвимости критического уровня риска были обнаружены в программных и аппаратных продуктах 23 вендоров.

Но опасность уязвимости — не единственный показатель значимости проделанной работы. ПО, в котором наши эксперты выявляют уязвимости, является системообразующим в инфраструктурах крупнейших компаний во всем мире. Это лидеры в своих нишах. Возникновение любой уязвимости в одном из ключевых программных продуктов в один момент ставит под удар миллионы компаний. Ниже приведены лишь несколько примеров, которые наглядно демонстрируют масштабы проблемы.

VPN-доступ для хакеров

В 2020 году эксперты Positive Technologies выявили и помогли устранить две опасные уязвимости в межсетевом экране Cisco ASA. Стоит отметить, что на момент публикации уязвимостей из интернета было доступно более 220 000 устройств, недостатками в которых потенциально могли воспользоваться хакеры. Используя первую уязвимость, неавторизованный внешний злоумышленник мог провести DoS-атаку на устройства и отключить VPN. То есть лишить треть российских компаний возможности удаленной работы сотрудников. Сейчас, когда многие компании сохранили режим удаленной работы для своих сотрудников, эта проблема может оказать значительное влияние на бизнес-процессы. Кроме того, VPN часто используется для организации связи между филиалами в распределенной корпоративной сети, а значит может нарушиться работоспособность ключевых систем, например ERP или электронной почты. Используя другую уязвимость, хакеры могли прочитать из памяти устройства cookie пользователя, подключенного по VPN, указать украденный идентификатор в клиенте Cisco VPN и попасть во внутреннюю сеть компании. Таким образом, компания могла быть скомпрометирована удаленно.

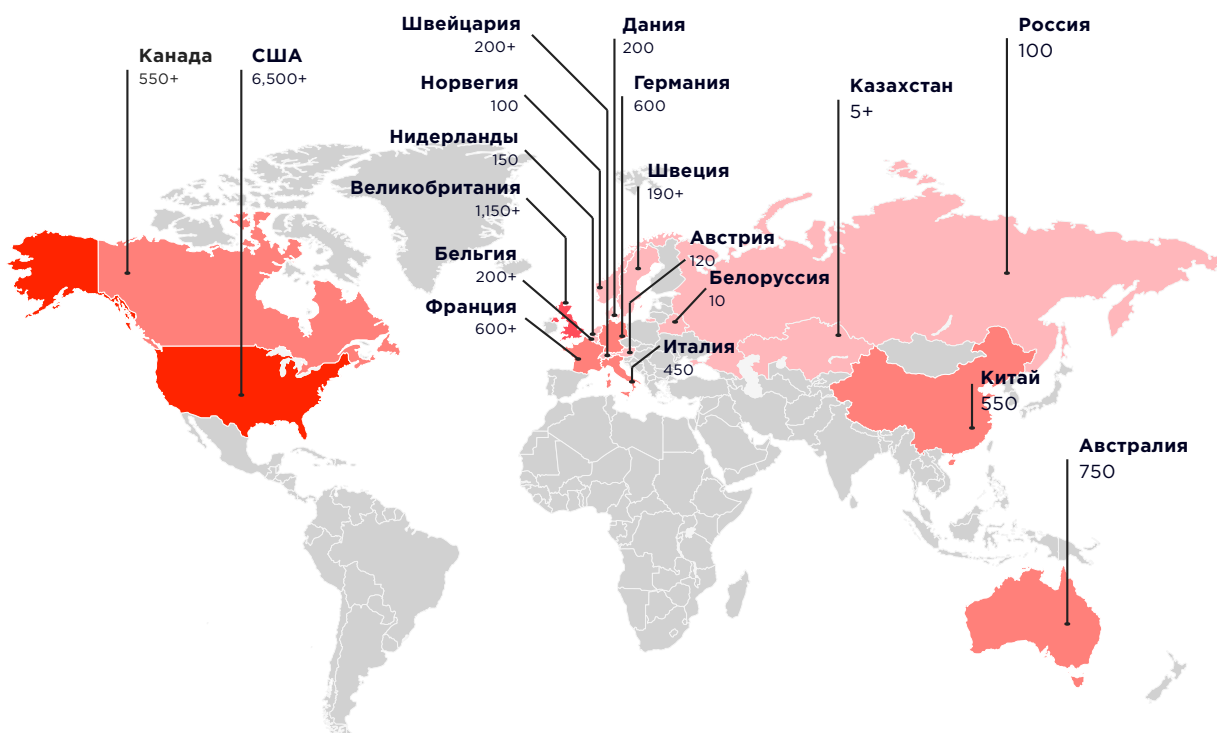
Нередко уязвимости выявляются в решениях, которые предназначены для защиты. Например, наши эксперты помогли устранить ошибки в ПО ведущих производителей:

- межсетевых экранах SonicWall (занимает пятое место на рынке аппаратных средств);
- системе управления уязвимостями Rapid7 (является ведущим поставщиком средств аналитики и автоматизации безопасности);
- операционной системе PAN-OS, используемой межсетевыми экранами следующего поколения (NGFW) Palo Alto Networks (является одним из лидеров в области ИБ);
- межсетевых экранах для защиты веб-приложений FortiWeb производства компании Fortinet (занимает первое место по количеству проданных средств безопасности и обеспечивает защиту более 415 000 клиентов по всему миру).

Прямой доступ во внутреннюю сеть за одну минуту

Еще одну критически опасную уязвимость, позволяющую любому внешнему нарушителю проникнуть во внутреннюю сеть компании менее чем за одну минуту, наши исследователи ИБ обнаружили в продуктах Citrix. Приложения Citrix широко применяются в корпоративных сетях, в том числе для удаленного подключения к рабочим компьютерам и критически важным бизнес-системам (например, ERP) с любого устройства через интернет. Данная уязвимость позволяет внешнему неавторизованному злоумышленнику не только получить доступ к опубликованным приложениям, но и проводить атаки с сервера Citrix на другие ресурсы внутренней сети атакуемой компании. По нашим оценкам, **уязвимы не менее 80 000 компаний из 158 стран**. Это значит, что если бы злоумышленники успели обнаружить этот недостаток раньше, чем было выпущено обновление ПО, то все эти компании в один момент оказались бы под угрозой компрометации. Мы рекомендуем организациям серьезно относиться к вопросам безопасности и проверять актуальность обновлений безопасности для используемого ПО.

Уязвимый Citrix: каждая пятая компания в мире все еще под угрозой



Распространение уязвимости
Количество уязвимых компаний:



© Positive Technologies

Возможности для продвижения хакера внутри корпоративной инфраструктуры

За первые четыре месяца 2021 года наши эксперты выявили семь уязвимостей в продуктах VMware, половина из которых критически опасны. К примеру, наиболее опасная уязвимость в ПО для управления виртуальной инфраструктурой VMware vCenter Server позволяет неавторизованному пользователю выполнять произвольные команды на сервере. После успешной эксплуатации данной уязвимости хакер может развить атаку, успешно продвинуться по корпоративной сети и получить доступ к данным, хранящимся в атакуемой системе (информации о виртуальных машинах, о пользователях и т. п.). Если же доступ к уязвимому ПО есть из глобальной сети (а число доступных из интернета и содержащих уязвимости устройств VMware vCenter во всем мире превышает 6000), то это позволяет внешнему злоумышленнику проникнуть в корпоративную инфраструктуру компании и также получить доступ к конфиденциальной информации. Стоит также отметить, что продукты компании VMware занимают до 80% рынка виртуализации, их используют более четырех миллионов пользователей и 20 000 компаний по всему миру.

Удаленное управление серверами

Раньше для администрирования серверов (например, установки обновлений, настройки ПО) требовалось физическое присутствие специалиста: необходимо было подключить к серверу монитор, клавиатуру и мышь — и лишь затем выполнять необходимые действия. Сегодня для этих целей используются веб-интерфейсы, доступные из любой точки мира. Одно из устройств для удаленного администрирования — Cisco Integrated Management Controller. За последние три года в нем были обнаружены и исправлены две критически опасные уязвимости, одну из которых нашли эксперты Positive Technologies. Она позволяла удаленно получить доступ к уязвимой системе и выполнять произвольные действия в ней с максимальными привилегиями, а значит — во всех компаниях, которые на момент выхода обновления использовали такие системы, злоумышленники могли захватить полный контроль над серверной инфраструктурой прямо из интернета.

Доступ к зашифрованным данным

Эксперты Positive Technologies уже несколько лет помогают компании Intel устранять недостатки в безопасности. Одна из уязвимостей была обнаружена в 2019 году в подсистеме Intel CSME, применяемой для удаленного обслуживания компьютеров. Внутри прошивки Intel CSME реализована схема удаленной аттестации доверенных систем, называемая Enhanced Privacy ID (EPID), которая позволяет однозначно и анонимно идентифицировать каждый конкретный компьютер. Злоумышленник, воспользовавшийся этой уязвимостью, может получить доступ к зашифрованным данным и не только их расшифровать, но и выдать свой компьютер за компьютер жертвы, обманув систему проверки подлинности. Отметим, что схема EPID используется также для защиты цифрового контента, обеспечения безопасности финансовых транзакций, аттестации IoT-устройств. Уязвимость присутствует в большинстве чипсетов Intel, выпущенных за последние пять лет. А поскольку микропрограммное обеспечение уже «зашито» в бортовой памяти чипсетов, то и исправить в нем уязвимости с помощью обновления прошивки невозможно: необходима замена чипсета.

Остановка технологического процесса

Мы видим, что за последние годы значительно увеличилось количество уязвимостей в сетевом промышленном оборудовании — в коммутаторах, конвертерах интерфейсов, шлюзах. Согласно отчету компании [Claroty](#), специализирующейся на промышленной кибербезопасности, в 2020 году было выявлено на 24,7% больше уязвимостей в АСУ ТП, чем годом ранее.

Эксперты Positive Technologies помогли компании Siemens выявить и устранить 23 уязвимости высокого и критического уровня опасности в 2018—2021 годах. В их число входят, например, недостатки в процессорном модуле программируемых логических контроллеров Siemens серии SIMATIC S7-1500, используемых для автоматизации технологических процессов на предприятиях пищевой промышленности, автомобильных заводах, в нефтехимии и в других отраслях. Уязвимости позволяли неавторизованному злоумышленнику полностью заблокировать работу ПЛК и остановить связанный с ними технологический процесс, вызвав тем самым остановку производства, порчу оборудования или аварию. Такие последствия могут в любой компании привести к колоссальным убыткам.

Полный контроль над оборудованием

В 2020 году наши специалисты обнаружили уязвимость наивысшего уровня опасности в контроллере доставки приложений BIG-IP, который используют в крупнейших компаниях по всему миру. Используя эту ошибку, злоумышленник, имеющий доступ к утилите BIG-IP, мог получить возможность выполнения команд и полностью скомпрометировать систему. Хакер мог создавать или удалять файлы, отключать службы, перехватывать информацию, выполнять произвольные системные команды и произвольный Java-код, а также мог развить атаку на внутренний сегмент сети. Особой опасности подвергались компании, у которых веб-интерфейс F5 BIG-IP был доступен из интернета: таких устройств на момент публикации уязвимости в июне 2020 года насчитывалось свыше 8000.

Списание произвольных сумм с банковских карт

Опасные уязвимости были обнаружены экспертами Positive Technologies в POS-терминалах компании Verifone, одного из крупнейших в мире поставщиков платежных терминалов (7,6 млрд транзакций ежегодно). Злоумышленники могли воспользоваться этими уязвимостями для перехвата PIN-кодов банковских карт, подмены информации о сумме транзакции на экране терминала, отправки в банк-эквайер запроса на списание произвольной суммы и других атак в 150 странах мира, где используются данные устройства. Учитывая масштабы краж карточных данных по всему миру и нацеленность преступников на сферу финансов, мошенничество с таким уязвимым терминалом сулило банкам и их клиентам ощутимые убытки.

Мы описали лишь часть наиболее серьезных проблем безопасности, которые наши специалисты выявляют регулярно в рамках своей работы. Мы перечислили примеры программных и аппаратных продуктов, знакомых всем IT-специалистам, ведь большинство ежедневно работают с ними в организациях по всему миру. Эти продукты играют очень важную роль, без них невозможно вести бизнес. Можно предположить, к каким последствиям могли бы привести атаки на организации, в которых эти продукты остались бы уязвимы. Злоумышленники не стоят на месте и регулярно модернизируют свои атакующие инструменты, а значит без постоянного сотрудничества производителей ПО с экспертами по ИБ невозможно победить в противостоянии с преступниками. Без активистов-исследователей каждому вендору пришлось бы в одиночку сражаться с натиском хакеров. Тогда процесс выявления и устранения уязвимостей превратился бы в поспешное реагирование на кибератаки и принятие мер по устранению последствий. Компании, использующие уязвимое ПО, теряли бы доверие к производителям и постоянно находились бы в поиске более безопасных альтернатив.

Эксперты Positive Technologies прилагают огромные усилия, чтобы сделать нашу технологическую среду безопасной. Мы ежедневно ведем общение с производителями программных и аппаратных решений — помогая им улучшить продукты, с исследователями — разделяя наши знания и экспертизу (придерживаясь принципов ответственного разглашения), с обычными пользователями — обучая их жизни в опасном киберпространстве. Это тот вклад в жизнь мирового сообщества ИБ, который обязана вносить каждая исследовательская компания, занимающаяся кибербезопасностью. И мы не планируем останавливаться!

О компании

ptsecurity.com
pt@ptsecurity.com
[facebook.com/
PositiveTechnologies](https://facebook.com/PositiveTechnologies)
facebook.com/PHDays

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте ptsecurity.com.