СТАТИСТИКА УЯЗВИМОСТЕЙ В 2011 ГОДУ

POSITIVE TECHNOLOGIES

ОГЛАВЛЕНИЕ

1 Введение

Портал по информационной безопасности SecurityLab.ru опубликовал отчет, содержащий статистику компьютерных уязвимостей за 2011 год. В центре внимания исследователей оказались SCADA-системы, CMS, программы компании Adobe, почти все браузеры и семейство операционных систем Windows. Данные приложения и системы в минувшем году часто становились доступными для проникновений. В этом обзоре мы расскажем о нескольких глобальных происшествиях, ставших результатом безобидных (на первый взгляд) уязвимостей, и приведем ряд статистических выкладок.

Уязвимости как способ остановить завод и ядерную программу

В 2011 году специалисты в полный голос заговорили о наступлении эпохи холодной кибервойны. Мишенями хакеров становятся промышленные предприятия и военные секреты. Например, осенью стало известно о троянском вирусе по имени Duqu. Он проникает в компьютер под управлением Windows, используя критическую уязвимость CVE-2011-3402. Затем вирус способен внедриться в смежную SCADA-систему предприятия с целью похищения информации об ИТ-инфраструктуре и установления контроля над промышленными объектами. Некоторые эксперты отмечали, что фрагменты основного модуля Duqu имеют большое сходство с «червём» Stuxnet, который в 2010 г. вывел из строя несколько иранских заводов по обогащению урана.

Поддельные SSL-сертификаты — месть за Иран?

Весной и летом 2011 г. иранские хакеры последовательно взломали серверы удостоверяющих центров Comodo и DigiNotar. Второй случай выдался особенно урожайным. Часть из украденных сертификатов безопасности принадлежали ЦРУ, Моссаду и MI-6. Помимо международной кибербразведки, похищенные «цифровые паспорта» использовались для атак man-in-the-middle (MitM). Хакер пропускал интернет-траффик «клиента» через собственный прокси-сервер, где браузер жертвы встречался с фальшивым сертификатом и выдавал информацию в расшифрованном виде. Под ударом оказались пользователи интернет-банкинга, почтовых онлайн-служб и других сервисов, использующих SSL-сертификаты.

Цифровые подписи и военные секреты США

Взломав сервера компании RSA Security в середине марта 2011 г., неизвестные хакеры поставили под угрозу надежность цифровых подписей RSA SecurID. Этими ключами пользовались более 40 млн. работников для получения доступа к закрытым сетям. Атака началась с электронного письма, призывающего работников головной компании RSA открыть фальшивый файл Excel с интригующим названием «План комплектования штата 2011.xls». Зараженная таблица при открытии устанавливала на ПК бекдор Poison Ivy, эксплуатируя уязвимость CVE-2011-0609 в Adobe Flash Player. Среди похищенной информации были сведения о новейших решениях для двухфакторной проверки подлинности.

Позже с помощью украденных ключей пытались взломать серверы крупнейшего в мире предприятия ВПК, корпорации Lockheed Martin.

Что бывает из-за несоответствия стандарту PCI DSS

В мае 2011 года были пойманы румынские хакеры, взломавшие системы обработки транзакций торговых терминалов и три года перехватывавшие данные платёжных карт клиентов. Основной удар

пришелся по компании Subway. Проникновение в ЛВС Subway, согласно информации The Wire, осуществлялось через беспроводные сети в ресторанах, а сами терминалы не соответствовали стандартам безопасности индустрии платёжных карт (PCI DSS). Кроме того, специалисты, осуществляющие удаленную техподдержку терминалов, не только не устанавливали обновления для приложения удалённого администрирования PCAnywhere, но и выбрали простейшую комбинацию логина и пароля (administrator, computer) в более чем 200 системах.

2 Состояние уязвимостей по наличию исправлений

Рис. 1. Состояние уязвимостей по наличию исправлений.

Всего за год было описано 4733 уязвимостей. Производители программного обеспечения смогли устранить к 1 января только 58% уязвимостей, а еще для 7% выпустили инструкцию по устранению. Таким образом, больше трети уязвимостей оставались открытыми для киберпреступников.

3 Распределение уязвимостей по типам воздействия

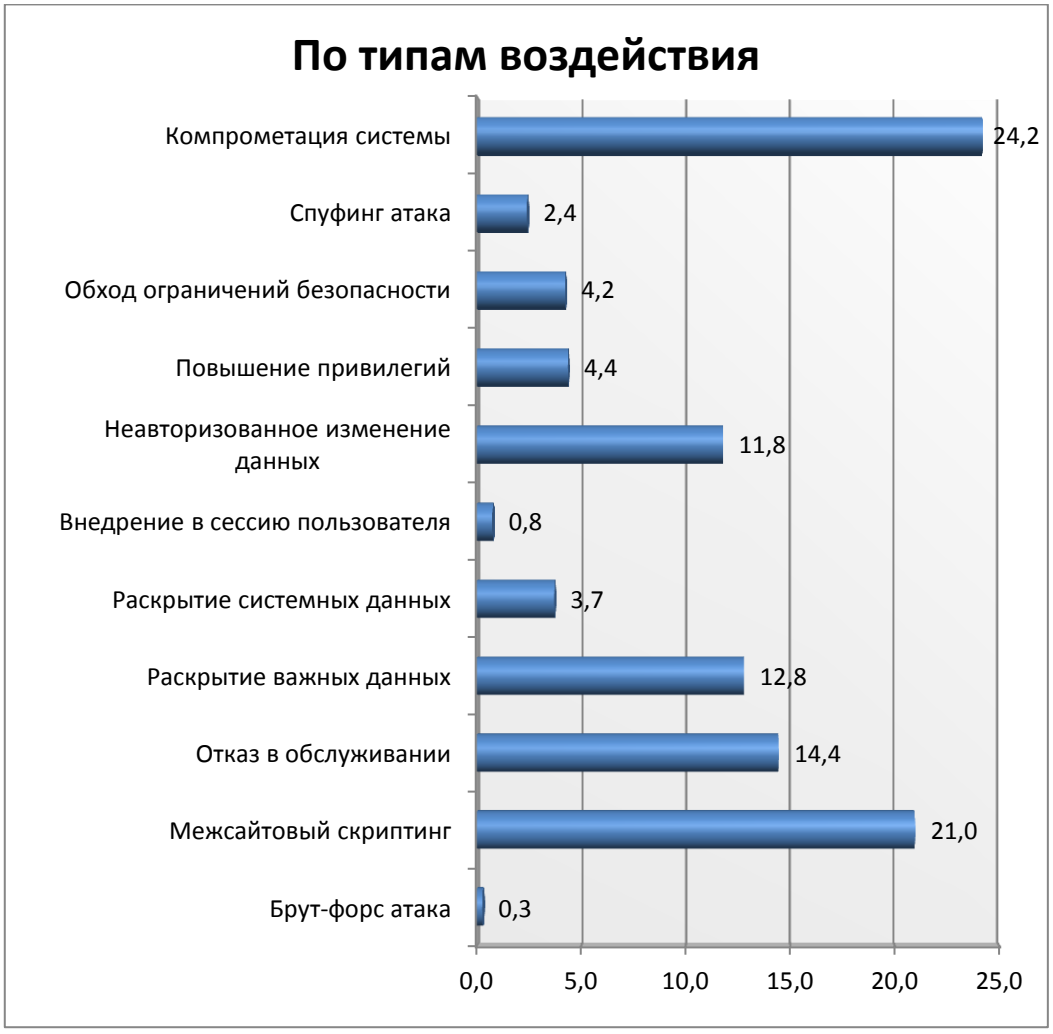

Рис. 2. Распределение уязвимостей по типам воздействия

Примерно четверть уязвимостей (24%) позволяли хакеру осуществить компрометацию системы, выполнив произвольный код на компьютере жертвы. Еще 21% обнаруженных «дыр» подходили для XSS-нападения, 15% могли быть использованы для отказа в обслуживании, 13% — для раскрытия важных данных, 12% — для неавторизованного изменения данных.

4 По вектору эксплуатации

Рис. 3. Уязвимости по вектору эксплуатации

Если рассмотреть все уязвимости за 2011 год, то злоумышленник мог работать удаленно при эксплуатации 77% уязвимостей. Для 15% требовалась локальная сеть, а для 8% — личное присутствие или инсайдерская информация.

5 Уязвимости по типам программного обеспечения

Мы бы хотели обратить внимание на уязвимости в следующих типах программного обеспечения.

Серверное ПО

Тип ПО/Опасность	Высокая	Средняя	Низкая
SCADA-системы	1	24	12
DNS-серверы	2	7	0
Web-серверы	2	9	13
Серверы приложений	3	5	22

Табл.1. Уязвимости в серверном ПО

В серверном программном обеспечении широкое распространение получили уязвимости в SCADA-системах: в 17 уведомлениях безопасности было описано 37 уязвимостей. Интерес исследователей к программной части АСУ ТП неслучаен — именно в последние два года получили распространение вирусы, нацеленные на приложения для промышленной автоматизации.

Уязвимости в клиентском ПО

Тип ПО/Опасность	Критическая	Высокая	Средняя	Низкая
Браузеры	4	425	77	88
Офисные приложения	3	127	7	16
Мультимедийные приложения	0	247	13	10
ActiveX компоненты	3	83	5	11

Табл. 2. Уязвимости в клиентском ПО

Уязвимости в браузерах

В 2011 году было обнаружено 594 уязвимости в самых популярных браузерах. Ниже представлена сводная таблица по уязвимостям в популярных браузерах. *Примечание:* При учете уязвимостей в браузерах во внимание не брались ошибки отказа в обслуживании.

Браузер	Уязвимостей	Критических	Высоких	Средний	Низких
Apple Safari	169	0	140	13	16
Chrome	278	1	197	42	38
Firefox	89	0	65	12	12
Internet Explorer	39	3	20	3	13
Opera	19	0	3	7	9

Табл. 3. Уязвимости в браузерах

Таким образом, по количеству уязвимостей лидером в 2011 году стал Google Chrome. На втором месте — Apple Safari, на третьем — Firefox.

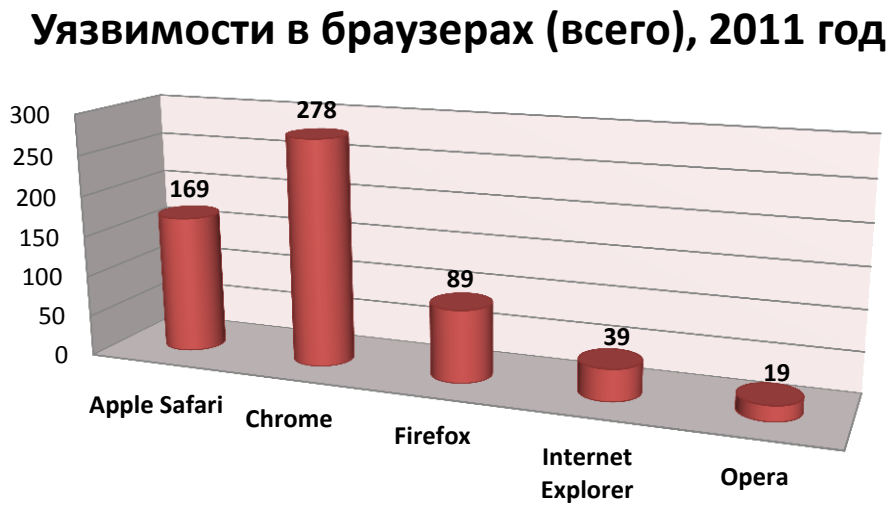

Рис. 4. Уязвимости в браузерах

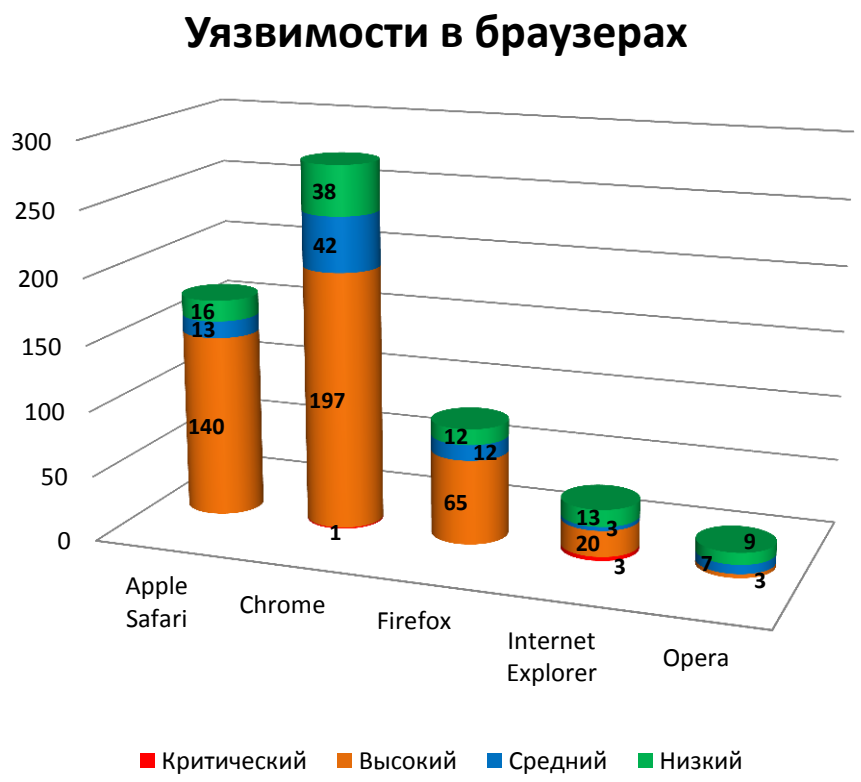

Рис. 5. Распределение уязвимостей в браузерах по уровню опасности

Самым защищённым браузером с точки зрения количества уязвимостей в 2011 стал Opera. Во всех распространенных приложениях этого типа, кроме Opera, было обнаружено очень большое количество уязвимостей высокой степени опасности, которые могут использоваться для компрометации системы. В минувшем году у ведущих браузеров было также найдено 4 уязвимости критической степени опасности, которые использовались злоумышленниками для проведения успешных атак на различные компании. Большинство из них (три) пришлись на Internet Explorer и одну обнаружили в Chrome 11.x.

Общее представление данных по уязвимостям в различных версиях браузеров выглядит

следующим образом:

Браузер/уровень опасности	Критический	Высокий	Средний	Низкий
Apple Safari 5.x	0	140	13	16
Chrome 8.x	0	16	4	2
Chrome 9.x	0	43	8	3
Chrome 10.x	0	23	3	4
Chrome 11.x	0	12	5	2
Chrome 12.x	1	26	9	1
Chrome 13.x	0	40	9	3
Chrome 14.x	0	17	2	8
Chrome 15.x	0	20	1	16
Internet Explorer 6	3	16	2	11
Internet Explorer 7	3	15	2	12
Internet Explorer 8	2	17	3	11
Internet Explorer 9	1	14	2	10
Mozilla Firefox 3.5.x	0	18	3	3
Mozilla Firefox 3.6.x	0	34	6	4
Mozilla Firefox 4.0.x	0	11	0	3
Mozilla Firefox 5.0.x	0	7	1	1
Mozilla Firefox 6.0.x	0	7	1	1
Mozilla Firefox 7.0.x	0	5	1	2
Mozilla Firefox 8.0.x	0	4	1	2
Opera 10.x	0	1	1	4
Opera 11.x	0	3	7	8
Opera Mobile for Android 11.x	0	0	0	1

Табл. 4. Уязвимости в разных версиях популярных браузеров

Уязвимости в популярных мультимедийных проигрывателях.

ПО/Опасность	Критическая	Высокая	Средняя	Низкая
Apple iTunes	0	133	1	3
Apple Quicktime	0	27	0	2
RealPlayer 14.x	0	22	0	0
VLC Media Player	0	14	1	0
Winamp	0	17	0	0
Windows Media Player	0	2	0	0

Прошлогодний хит-парад наиболее уязвимых медиа-проигрывателей (из числа популярных) возглавил Apple iTunes (133 уязвимости). В середине списка идет распространённый VLC Media Player (15 уязвимостей), а у Windows Media Player было опубликовано всего две уязвимости, что примерно в 70 раз меньше, чем у Apple iTunes.

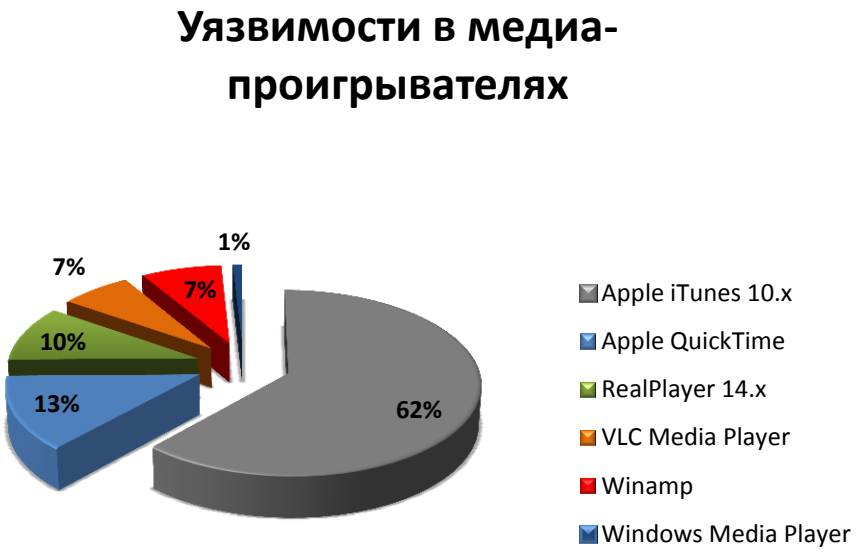

Рис. 6. Уязвимости в популярных мультимедийных проигрывателях.

6 Уязвимости «нулевого дня»

Уязвимости «нулевого дня» — головная боль для разработчиков. Эти бреши в системе активно эксплуатируются хакерами еще до публикации сообщения об уязвимости и выхода патча.

Любопытно отметить рост числа таких уязвимостей в продуктах Adobe — в минувшем году их было найдено семь, и по этому параметру Adobe обогнала другого гиганта — компанию Microsoft, у которой было 5 уязвимостей «нулевого дня». В числе свежих примеров — обнаруженная в конце 2011 г. уязвимость CVE-2011-2462 в Adobe Reader, использовавшаяся для взлома подрядчика министерства обороны США ManTech.

Приложение	Уязвимости
Flash Player	3
Internet Explorer	3
Microsoft Windows	2
Adobe Reader	3
Yahoo! Messenger	1
ISC BIND	1
Hancom Office	1

Табл. 4. Уязвимости нулевого дня

В следующей таблице представлена сравнительная статистика по уязвимостям нулевого дня для Microsoft и Adobe.

Производитель	2006	2007	2008	2009	2010	2011
Microsoft	6	3	5	6	6	5
Adobe	0	0	1	4	7	7
Другие	1	0	0	3	0	3

Табл. 5. Уязвимости нулевого дня для Microsoft и Adobe.

Рис. 7. График уязвимостей нулевого дня с 2005 года

7 Уязвимости в операционных системах

Популярность Windows логичным образом сказывается на количестве уязвимостей. По сравнению с другими операционными системами, у продукта от Microsoft их было найдено больше всего. Причем, линейка ОС Windows держит лидерство как в общем зачете (92 уязвимости), так и в индивидуальном — только у этих ОС в отчетный период было обнаружено две критические уязвимости. С другой стороны, максимальное число уязвимостей высокой степени опасности (33) обнаружили в Mac OS, у Windows их нашли 22, а в разных версиях Linux — всего одну. При учете уязвимостей во внимание не принимались уязвимости в ПО сторонних производителей.

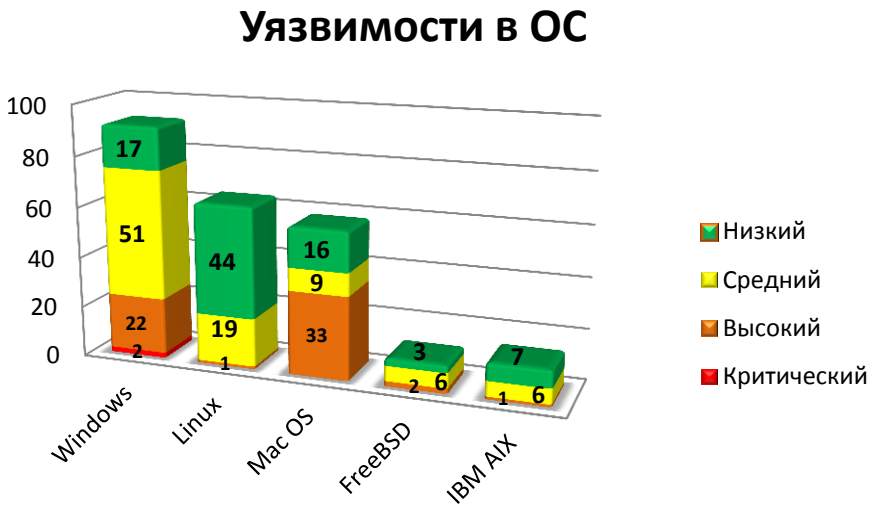

Рис. 8. График уязвимостей в операционных системах по степени опасности

8 Уязвимости в Web-приложениях

Наилучшие условия для несанкционированных проникновений в сегменте веб-приложений предоставляют системы управления содержимым (18%) . Хакеры постоянно ищут уязвимости в CMS, и, как мы видим, находят их в большом количестве (204 уязвимости за год). Администраторам сайтов, построенных на популярных платформах, необходимо не только контролировать подозрительную активность, но и оперативно устанавливать обновления для CMS. Следует не забывать также о веб-форумах, которые идут на втором месте по количеству уязвимостей (7%).

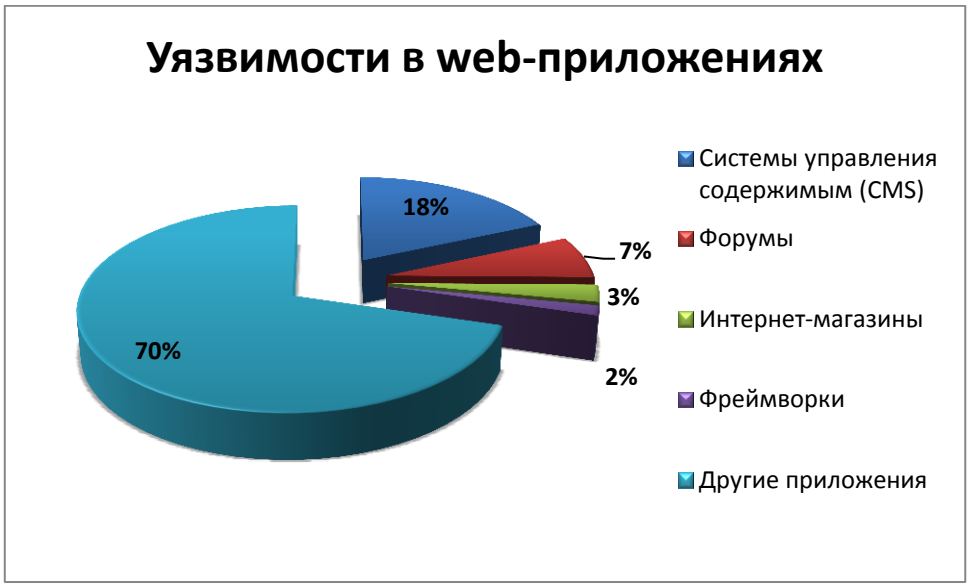

Рис. 9. Распределение уязвимостей в Web-приложениях

9 Справочник

Типы воздействий

При описании уведомлений безопасности SecurityLab использует следующие типы воздействий:

Брут-форс атака (атака грубой силы)
Это воздействие используется, когда приложение или алгоритм позволяет атакующему осуществить подбор логина/пароля, или других данных, используемых для ограничения доступа к ресурсам приложения.

Межсайтовый скриптинг
Подобные уязвимости позволяют злоумышленнику изменить поведение или содержимое страниц веб-приложения в браузере целевого пользователя. К этому типу относятся все уязвимости, связанные с выполнением сценариев в браузере (хранимый и отраженный XSS, CSRF, расщепление HTTP запросов и пр.).

Отказ в обслуживании
К этому типу воздействия относятся уязвимости, которые позволяют злоумышленнику нарушить корректную работу и повлиять на доступность приложения или ОС.

Раскрытие важных данных
Этот тип воздействия используется для определения уязвимостей, которые позволяют атакующему получить доступ к документам, файлам, учетным данным пользователей или другой потенциально важной информации.

Раскрытие системных данных
К этому типу относятся уязвимости, которые позволяют злоумышленнику получить системные данные (версию ОС, запущенные службы, месторасположение файлов на системе).

Внедрение в сессию пользователя
К этому типу относятся уязвимости, которые позволяют злоумышленнику внедриться в сессию пользователя в приложении и выполнить некоторые действия от его имени.

Неавторизованное изменение данных
К этому типу относятся уязвимости, которые позволяют атакующему произвести изменение данных, не имея требуемых привилегий доступа, например, используя SQL-инъекцию в приложении.

Повышение привилегий
К этому типу воздействия относятся уязвимости, которые позволяют локальному пользователю получить привилегии другой учетной записи в системе.

Обход ограничений безопасности
К этому типу воздействия относятся уязвимости, которые позволяют злоумышленнику обойти определенные механизмы безопасности приложения.

Спуфинг атака
Этот тип обозначает уязвимости, которые позволяют злоумышленнику выдать себя за другого пользователя или систему.

Компрометация системы
К этому типу воздействия относятся уязвимости, которые позволяют удаленному пользователю выполнить произвольный код на целевой системе с привилегиями пользователя или уязвимой службы.

Степень опасности уязвимостей
При публикации уведомлений SecurityLab оценивает рейтинг опасности уязвимостей согласно нижеописанным критериям. При этом во внимание принимается рейтинг CVSSv2.

Критическая степень опасности
К этому типу опасности относятся уязвимости, которые позволяют удаленную компрометацию системы без дополнительного воздействия целевого пользователя и активно эксплуатируются на момент публикации первого сообщения об уязвимости, т.е. являются уязвимостями «нулевого дня». Таким образом, критическими считаются уязвимости с CVSSv2 рейтингом >=8.7, которые стали известны вследствие происшедшего инцидента безопасности.

Высокая степень опасности
К этому типу опасности относятся уязвимости, которые позволяют удаленную компрометацию системы. Уязвимости с CVSSv2 рейтингом >=7.4 считаются уязвимостями высокой степени опасности.

Средняя степень опасности
К этому типу относятся уязвимости, которые позволяют удаленный отказ в обслуживании, неавторизованный доступ к данным или выполнение произвольного кода при взаимодействии пользователя (например, подключение к злонамеренному серверу уязвимым приложением). CVSSv2 рейтинг >= 4.7.

Низкая степень опасности
К этому типу относятся все уязвимости, эксплуатируемые локально, также уязвимости, эксплуатация которых затруднена или которые имеют минимальное воздействие (например, XSS, отказ в обслуживании клиентского приложения). CVSSv2 рейтинг < 4.7.

9 Исследовательский центр Positive Research

Positive Research – один из крупнейших в Европе исследовательских центров в области информационной безопасности. Он является инновационным подразделением компании Positive Technologies, ключевого эксперта в сегменте практических аспектов защиты информации.

С 2004 года при содействии Positive Research лидеры ИТ-отрасли, среди которых Microsoft, Cisco, Google, Avaya, Citrix, VmWare, Trend Micro, устранили несколько сотен уязвимостей и недочетов систем безопасности.