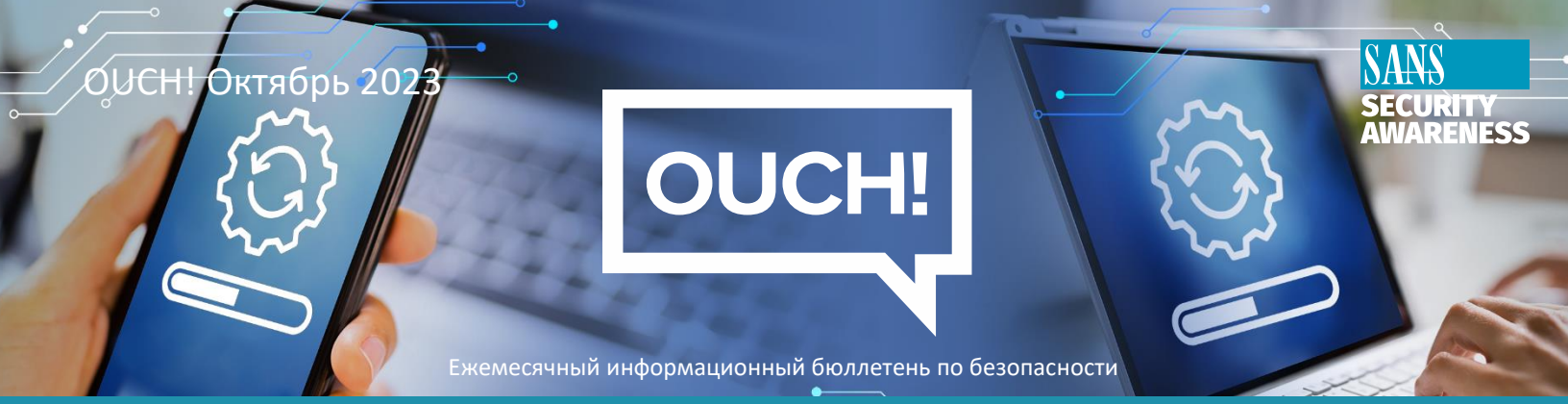
OUCH! Октябрь 2023



Сила обновления

Обзор

Кибер-злоумышленники постоянно ищут и находят новые уязвимости в программном обеспечении, которое вы используете каждый день. Уязвимость — это ошибка или слабость в разработке программного обеспечения. Это программное обеспечение может запускать ваш ноутбук, мобильные приложения на вашем смартфоне или, возможно, даже программное обеспечение в вашем термостате. Кибер-злоумышленники пользуются этими уязвимостями программного обеспечения и используют их, что позволяет им удаленно взламывать системы, в том числе используемые вами. В то же время поставщики программного обеспечения и устройств постоянно разрабатывают исправления этих недостатков и выпускают исправления в виде обновлений программного обеспечения. Один из лучших способов защитить себя — убедиться, что используемые вами технологии всегда имеют последние обновления. Эти обновления не только устраняют известные уязвимости, но и часто добавляют новые функции безопасности, что значительно затрудняет взлом ваших устройств кибер-злоумышленникам.

Как работает обновление

Когда об уязвимости программного обеспечения становится известно, разработчик или поставщик создает программное исправление для этой уязвимости (называемое патчем) и публикует обновление. Затем ваша система загружает и устанавливает это обновление, устраняя уязвимости. Примеры программного обеспечения, которое необходимо обновить:

- Операционные системы, на которых работает ваш ноутбук (например, Microsoft Windows или Apple OSX) или на вашем смартфоне (например, Android или iOS)
- Домашнее сетевое оборудование, такое как интернет-маршрутизатор или точки доступа Wi-Fi, или домашние интеллектуальные устройства, такие как термостаты, дверные звонки, бытовая техника или камеры видеонаблюдения.
- Программы, которые работают на ваших устройствах, например веб-браузер вашего ноутбука или мобильные приложения вашего телефона.

Вот почему, когда вы покупаете новую компьютерную программу или новое мобильное приложение, сначала убедитесь, что поставщик программного обеспечения активно обновляет программу или устройство. Чем дольше программное обеспечение работает без обновлений, тем больше вероятность того, что в нем есть уязвимости, которыми могут воспользоваться злоумышленники. Вот почему многие поставщики, такие как Microsoft, автоматически выпускают новые исправления каждый месяц. Кроме того, если вы больше не используете определенную компьютерную программу, программное обеспечение или мобильное приложение, удалите их из своей системы.

Чем меньше программного обеспечения вы установили, тем меньше у вас потенциальных уязвимостей и тем выше ваша безопасность. Наконец, если какие-либо из ваших устройств или приложений устарели и больше не поддерживаются поставщиком, мы рекомендуем вам заменить их более новыми версиями, которые активно обновляются и поддерживаются.

Как обновить

Есть два способа обновить вашу систему.

1. **Ручной (сложный способ)**: Когда обновление доступно, вы вручную загружаете и устанавливаете его. Это дает вам больше контроля над тем, как и когда устанавливаются обновления. Недостатком ручных обновлений является то, что это намного больше работы, поскольку вам нужно не только отслеживать, когда каждое из ваших устройств или программ должно быть обновлено, но и обновлять их вручную, что позволяет легко забыть об их обновлении.

2. **Автоматический (простой способ)**: Вы включаете автоматическое обновление на всех своих устройствах, что означает, что всякий раз, когда выпускается новый патч, ваше устройство автоматически загружает и устанавливает его. Преимущество автоматических обновлений в том, что большая часть работы выполняется за вас. Недостатком автоматического обновления является то, что обновленная программа может вызвать проблемы, приводящие к потере функциональности или данных. Это редкость для персональных устройств, но может случиться в более сложных средах, например, в крупных корпорациях. Когда вы включаете автоматические обновления, обязательно регулярно проверяйте свою систему, чтобы убедиться, что обновления происходят.

Из двух подходов мы настоятельно рекомендуем вам включить и использовать автоматическое обновление на всех ваших личных устройствах. Это гарантирует, что все технологии, которые вы используете, от вашего смартфона и ноутбука до радионяни и дверных замков, имеют новейшее программное обеспечение. Благодаря современным устройствам и программному обеспечению кибер-злоумышленникам намного сложнее взломать вас и ваши системы.

Приглашенный редактор

Доктор Джанелл Страх — преподаватель Университета Райса, где она преподает кибербезопасность и искусственный интеллект. Джанелл является председателем совета женщин в кибербезопасности (WiCyS). С доктором Страх можно связаться по адресу janell@wicys.org.

Ресурсы

Кибер-цифровая весенняя уборка: https://www.sans.org/newsletters/ouch/digital-spring-cleaning-7-simple-steps/
Нужно ли мне программное обеспечение для обеспечения безопасности?:
https://www.sans.org/newsletters/ouch/security-software/
Эмоциональные триггеры: как вас обманывают кибер-злоумышленники:
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Роман Полаков