Этические принципы «Лаборатории Касперского» по ответственному раскрытию уязвимостей

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Узнать больше на www.kaspersky.ru

Наша жизнь и общество стремительно меняются вместе с технологиями, которые становятся неотъемлемой частью нашего повседневного опыта. Однако в силу сложности современных технологий, ошибки, уязвимости и сбои становятся практически неизбежными. Именно мы – люди, которые разрабатывают технологии и которые их используют – несем ответственность за реагирование на непредвиденные обстоятельства и последствия. Мы твердо верим, что сбои и ошибки, которые неизбежно сопровождают развитие технологий должны быть исправлены всегда.

Чтобы создать здоровую и безопасную технологическую среду для общества, мы работаем с вендорами, исследователями, пользователями и другими заинтересованными сторонами, и придерживаемся при этом принципов процесса ответственного раскрытия уязвимостей (Responsible Vulnerability Disclosure, RVD), который призван снизить риск от неизбежных технологических ошибок.

В каждом отдельном случае, мы ставим безопасность наших пользователей – людей и организаций, использующих наши продукты и решения – на первое место, и поэтому сотрудничаем с вендорами – лицами или организациями, разработавшими или обслуживающими продукт, в котором обнаружена уязвимость, а также другими возможными ее жертвами. В нашей работе по раскрытию уязвимостей мы руководствуемся этическими принципами, которые определяют прозрачность, ответственность и последовательность наших действий, и на которых основаны наши внутренние политики и процессы.

#1 Укреплять доверие

Доверие – это основа любых взаимоотношений, и наша работа, в частности, невозможна без доверия. Невозможно представить без него и процесс ответственного раскрытия уязвимостей. Поэтому мы продолжим:

- ставить во главу угла интересы и безопасность пользователей и общества;
- сообщать обо всех найденных уязвимостях в первую очередь вендору, перед раскрытием информации о найденных уязвимостях;
- вести себя прозрачно и предсказуемо по отношению к участникам процесса, включая исследовательское сообщество, центры реагирования на инциденты и угрозы, государственные органы, и широкую общественность;
- исходить из принципа, что все участники процесса действуют из наилучших побуждений и прикладывают все усилия для координации действий и предотвращения использования уязвимости злоумышленниками.

#2 Информировать стороны, затронутые угрозой, в приоритетном порядке

Ответственное раскрытие уязвимостей - это комплексный процесс со множеством переменных: вендор, в продукте которого была найдена уязвимость, может не выходить на связь, у участников процесса могут смениться приоритеты, в конце концов, никто не застрахован от утечки данных об уязвимости. Но несмотря на все сложности, которые могут возникнуть в процессе, мы обязуемся продолжать:

- в первую очередь информировать о найденной уязвимости вендора и начинать координацию действий именно с него, чтобы содействовать устранению уязвимости и минимизации рисков, принимая при этом меры по защите собственных пользователей;
- предоставлять вендору проверенные и обоснованные данные о найденной уязвимости для принятия обдуманных и взвешенных решений;
- открыто и своевременно информировать все вовлеченные стороны о наших шагах, следуя лучшим практикам по ответственному раскрытию уязвимостей.

#3
Координировать усилия сторон

Когда в процесс вовлечено несколько сторон, как часто бывает при выявлении уязвимостей в продуктах компаний с глобальными цепочками поставок, крайне важно координировать действия. Поэтому мы продолжим:

- сотрудничать с внешними организациями в соответствии с передовыми практиками, принятыми в индустрии, включая международный стандарт ISO/IEC 29147:2018 по раскрытию уязвимостей;
- в зависимости от каждого конкретного случая, предоставлять всем сторонам время для тщательного анализа уязвимости и разработки плана ее устранения;
- призывать все заинтересованные стороны, включая независимых исследователей и экспертов в сфере кибербезопасности координировать и согласовывать свои действия.

#4
Сохранять конфиденциальность там, где это уместно

Если техническая информация о найденной уязвимости будет раскрыта раньше времени, она может помочь злоумышленникам и подвергнет риску пользователей. Поэтому все данные об уязвимостях мы передаем строго в конфиденциальном порядке вендору, соблюдая необходимые меры предосторожности и принципы разумности. Но если вендор не предпринимает меры по устранению уязвимости, нам придется сообщить об угрозе пользователям (не только нашим). Поэтому мы продолжим:

- конфиденциально передавать необходимую информацию сторонам, которые должны разрабатывать меры по устранению уязвимости;
- использовать самые надежные и безопасные каналы связи для передачи данных, чтобы гарантировать, что данные, имеющие непосредственное отношение к найденной уязвимости или инциденту, обрабатываются в соответствии с применимым законодательством, контрактными обязательствами, и сохранением приватности вовлеченных сторон;
- согласовывать условия публичного раскрытия информации об уязвимости с вендором в соответствии с его политикой по раскрытию уязвимостей и следуя требованиям местного законодательства;
- если вендор не отвечает, а уязвимость крайне опасна и может затронуть большее количество пользователей в ближайшей перспективе, нам приходится раскрывать информацию о ней через собственные каналы информации и СМИ в соответствии с нашей внутренней политикой, локальным регулированием и передовыми индустриальными практиками, проинформировав вендора о нашем намерении.

#5
Поощрять ответственное поведение

Индустрия, государства и пользователи всё больше осознают важность ответственного раскрытия найденных уязвимостей. Мы верим, что очень важно поощрять ответственное поведение в этой области и в этой связи продолжим:

- привлекать внимание к процессу ответственного раскрытия уязвимостей для формирования стандартов ответственного поведения в индустрии и, тем самым, обеспечить своевременное реагирование на обнаруженные уязвимости и разработку планов по ее устранению;
- открыто поддерживать тех, кто ответственно сообщает о найденных уязвимостях и следует принятым индустрией стандартам ответственного раскрытия уязвимостей.

О «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, 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 270 тысяч корпоративных клиентов во всем мире.

Узнать больше на www.kaspersky.ru.

www.kaspersky.ru

kaspersky

Enterprise Cybersecurity: www.kaspersky.com/enterprise
TechnoWiki: www.kaspersky.com/technowiki
IT Security News: www.kaspersky.com/blog
Cyber Threats News: www.securelist.com