Опыт взаимодействия с международным сообществом разработчиков при исправлении уязвимостей: ответственное разглашение, сроки исправления

Игнатов Егор Павлович, ООО «Базальт СПО», г. Москва, ул. Бутырская, д. 75, egori@basealt.ru
Кузнецов Александр Максимович, ООО «Базальт СПО», г. Москва, ул. Бутырская, д. 75, kuznetsovam@basealt.ru
Шашкин Александр Иванович, ООО «Базальт СПО», г. Москва, ул. Бутырская, д. 75, dutyrok@basealt.ru

Введение

После того, как уязвимость в свободном программном обеспечении была обнаружена и было разработано исправление, непростой задачей может оказаться его донесение до международного сообщества разработчиков. В данной работе на трех примерах рассмотрен опыт взаимодействия с международным сообществом разработчиков ядра Linux, библиотеки Libvirt и кэширующего прокси-сервера Squid, а также предложены рекомендации по организации данного взаимодействия.

Взаимодействие с международным сообществом разработчиков ядра Linux

Ядро Linux является важной частью IT сферы нашего мира. Тысячи людей из разных стран вовлечены в его разработку. И так случается, что над исправлением одной и той же ошибки могут работать несколько команд.

В нашей практике имеется аналогичный случай. После анализа срабатывания WARNING in vmci_datagram_dispatch, которое было обнаружено с помощью фаззинг-тестирования. Подготовленное нами исправление было отправлено в международное сообщество согласно руководству по отправке изменений в ядро [1] 27 декабря 2023 года. Чуть позже выяснилось, что при отправке в список получателей не был добавлен почтовый адрес рассылки linux-kernel@vger.kernel.org, а сопровождающие подсистемы просто проигнорировали данное письмо. 10 января 2024 года мы повторно отправили исправления уже с добавленным адресом рассылки. Однако сопровождающий стабильных веток ядра Linux ответил, что исправление этой ошибки уже было зарегистрировано ранее, 05 января, компанией Oracle. Предложенные ими изменения, который аналогичны нашим, в последствие приняли в исходный код ядра.

Несмотря на то, что оплошность, допущенная при отправке, была исправлена в течение 2 недель, наше участие не было учтено. Однако после дополнительного анализа в этой же подсистеме нами исправлен ряд аналогичных ошибок, и правки были приняты международным сообществом.

Взаимодействие с международным сообществом разработчиков прокси-сервер Squid

По результатам фаззинга прокси-сервера Squid была обнаружена уязвимость, эксплуатация которой могла привести к реализации атаки типа "отказ в обслуживании". В соответствии с процедурой ответственного разглашения Squid [2] и рекомендациями к структуре отчета об ошибке [3] сведения об этом были направлены в закрытый список рассылки squid-bugs.

В первичном отчете об ошибке нами не был установлен период эмбарго, и, хотя ответ с подтверждением уязвимости был получен в течении трех дней, уязвимость была непублично исправлена через 19 дней, выход обновленной версии, содержащей исправления, появился только через 5 месяцев, в течение которых мы не имели возможности каким-либо образом влиять на раскрытие сведений об уязвимости и устанавливать сроки раскрытия. В связи с этим, было принято решение о необходимости самостоятельно устанавливать период эмбарго на неразглашение информации об уязвимости.

Взаимодействие с международным сообществом разработчиков библиотеки Libvirt

По результатам фаззинга была обнаружена уязвимость, эксплуатация которой могла привести к реализации атаки типа "отказ в обслуживании". В соответствии с процедурой ответственного разглашения libvirt [4] и опираясь на опыт сообщения об уязвимости в Squid, а также Google Project Zero vulnerability disclosure FAQ [5] было направлено письмо, устанавливающее период эмбарго на неразглашение сведений об уязвимости в течение 90 дней. Уязвимости был присвоен индекс CVE-2024-1441 и информация о ней была публично опубликована через 23 дня после направления письма, с рекомендацией от разработчиков устанавливать более сжатые сроки эмбарго от 14 дней и меньше. Следующая аналогичная уязвимость была направлена с эмбарго в 14 дней, а публично опубликована через 21 день с двукратным продлением сроков эмбарго. Продление сроков эмбарго происходило по согласованию, тем не менее в течение 15-го и 21-го дня с момента направления письма подтверждения продления эмбарго еще не произошло, но срок первичного эмбарго уже истек. В связи с этим было принято решение о необходимости заранее определять порядок действий в случае истечения эмбарго, но при этом продлевать его при положительной реакции со стороны сообщества разработчиков.

Заключение

Таким образом, сформированы следующие рекомендации по выстраиванию взаимодействия с международным сообществом разработчиков в случае отправки информации об обнаруженной уязвимости:

1. Четко следовать процедуре ответственного разглашения, определенной для конкретного программного обеспечения.
2. Самостоятельно устанавливать период эмбарго на неразглашение информации об уязвимости.
3. Заранее определять и информировать разработчиков о порядке действий в случае истечения периода эмбарго. Периодически обозначать приближающееся истечение периода эмбарго.

Список литературы

1. Submitting patches: the essential guide to getting your code into the kernel // The Linux Kernel documentation [Электронный ресурс]. URL: https://www.kernel.org/doc/html/latest/process/submitting-patches.html свободный (дата обращения: 07.05.2024).
2. Squid Mailing lists [Электронный ресурс]. URL: https://www.squid-cache.org/Support/mailing-lists.html#squid-bugs (дата обращения: 07.05.2024).
3. Sending Bug Reports to the Squid Team | Squid Web Cache wiki [Электронный ресурс]. URL: http://wiki.squid-cache.org/SquidFaq/BugReporting (дата обращения: 07.05.2024).
4. libvirt: Security Process [Электронный ресурс]. URL: https://libvirt.org/securityprocess.html (дата обращения: 07.05.2024).
5. Project Zero: Vulnerability Disclosure FAQ [Электронный ресурс]. URL: https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html (дата обращения: 07.05.2024)