АНАЛИЗ УЯЗВИМОСТЕЙ ОПЕРАЦИОННЫХ СИСТЕМ НА БАЗЕ ЯДРА LINUX

Э.К. Мурадов, С.Ю. Павлович

Согласно данным Лаборатории Информационных технологий Национального Института стандартов и технологий США, к маю 2020 года было обнаружено 4017 уязвимостей в ядре Linux [1]. Эксплуатация более половины из обнаруженных уязвимостей приводит к отказу в обслуживании (нарушению доступности операционной системы на базе ядра Linux), более 15 % – к несанкционированному доступу к данным, более 10 % – к повышению привилегий пользователей системы. Причинами большого количества обнаруженных уязвимостей ядра Linux являются открытость его исходного кода и широкое применение. При этом следует заметить, что эти причины обуславливают возможность превентивного обнаружения уязвимостей и оперативного их устранения.

Уязвимости наиболее высокой степени информационного риска обусловлены следующими причинами.

1. Значение TCP_SKB_CB(skb)→tcp_gso_segs может быть переполнено целым числом в ядре Linux при обработке выборочных подтверждений TCP (SACK). Злоумышленник может использовать это удаленно для того, чтобы реализовать угрозу типа «отказ в обслуживании» [2].

2. Функция mq_notify в ядре Linux не устанавливает значение указателя сокета на NULL при входе в режим повторов. Во время закрытия сокета Netlink пользовательским пространством, злоумышленники могут организовать угрозу типа «отказ в обслуживании» [3]. Netlink – интерфейс ядра Linux для установки связи между пользовательскими процессами и процессами самого ядра.

3. В ядре Linux hns_roce_alloc_ucontext не инициализирует соответствующую структуру данных, что может позволить злоумышленникам реализовать несанкционированный доступ к информации из памяти стека ядра [4].

4. Реализация coredump в ядре Linux не использует блокировки или другие механизмы для предотвращения изменений макета vma или флагов vma во время работы, что позволяет локальным пользователям реализовать несанкционированный доступ к информации [5].

5. Функция vmacache_flush_all в mm/vmacache.c неправильно обрабатывает переполнения порядкового номера. Злоумышленник может инициировать use-after-free с помощью определенных операций создания потоков, сопоставления, отмены отображения, аннулирования [6].

6. Состояние гонки в kernel/events/core.c в ядре Linux позволяет локальным пользователям получать привилегии через специально созданное приложение, которое делает одновременные системные вызовы perf_event_open для перемещения группы программного обеспечения в аппаратный контекст [7].

Для снижения вероятности реализации угроз, связанных с эксплуатацией рассмотренных и ряда других уязвимостей, необходимо выполнять настройки безопасности используемой операционной системы на базе ядра Linux, уделяя при этом особое внимание настройке подключаемых модулей аутентификации (PAM-модулей), либо применять такую систему в защищенном исполнении (например, операционную систему специального назначения Astra Linux SE).

Литература

1. National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results _type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Alinux&cpe_product=cpe%3A%2F%3A%3Alinux_kernel. – Дата доступа: 10.05.2020.

2. CVE–2019–11477 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2019–11477. – Дата доступа: 10.05.2020.

3. CVE–2017–11176 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2017–11176. – Дата доступа: 10.05.2020.

4. CVE–2019–16921 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2019–16921. – Дата доступа: 10.05.2020.

5. CVE–2019–11599 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2019–11599. – Дата доступа: 10.05.2020.

6. CVE–2018–17182 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2018–17182. – Дата доступа: 10.05.2020.

7. CVE–2017–6001 Detail / National vulnerability database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE–2017–6001. – Дата доступа: 10.05.2020.