CISA добавляет в свой каталог новую ошибку, дающую хакеру полную свободу действий.

Агентство Cybersecurity and Infrastructure Security Agency (CISA) – это агентство, которое отвечает за защиту критической инфраструктуры США от киберугроз. Оно осуществляет мониторинг и анализ угроз, разрабатывает рекомендации по защите и обеспечивает техническую и информационную поддержку для организаций в этой отрасли. CISA также сотрудничает с другими правительственными агентствами и частным сектором для улучшения кибербезопасности в стране." data-html="true" data-original-title="CISA" >CISA добавило уязвимость ядра Linux в каталог известных эксплуатируемых уязвимостей (KEV), сославшись на доказательства активной эксплуатации.

CVE-2024-1086 (оценка CVSS 3.1: 7,8) связана с ошибкой use-after-free (UAF) в компоненте Netfilter – это фреймворк, встроенный в ядро Linux, который позволяет управлять сетевым трафиком на разных уровнях. Он используется для реализации брандмауэров, NAT, мониторинга и других функций." data-html="true" data-original-title="Netfilter" >netfilter и позволяет локальному злоумышленнику повысить привилегии обычного пользователя до root и выполнить произвольный код. Уязвимость была устранена в январе 2024 года. При этом точная природа атак, использующих уязвимость, на данный момент неизвестна.

Netfilter — это платформа, предоставляемая ядром Linux – это свободная и открытая операционная система, разработанная Линусом Торвальдсом в 1991 году. С тех пор Linux стал одной из наиболее популярных альтернатив коммерческим операционным системам.

 Основное преимущество Linux заключается в его открытом исходном коде, что позволяет пользователям свободно изменять и распространять систему в соответствии с лицензией GNU GPL.

 Linux предоставляет стабильную, надежную и гибкую платформу для работы с компьютером или сервером. Большинство дистрибутивов Linux (например, Ubuntu, Fedora, Debian) поставляются с разнообразными программами и инструментами для работы, включая офисные приложения, интернет-браузеры, мультимедийные инструменты и многое другое.

 Linux также широко используется в серверной сфере и встроенных системах, таких как маршрутизаторы и мобильные устройства." data-html="true" data-original-title="Linux" >Linux, которая позволяет реализовывать различные сетевые операции в виде пользовательских обработчиков для облегчения фильтрации пакетов, трансляции сетевых адресов и трансляции портов.

В каталог Known Exploited Vulnerabilities (KEV) — это каталог известных

эксплуатируемых уязвимостей, который ведётся агентством по кибербезопасности и защите инфраструктуры США (CISA). KEV представляет собой справочник уязвимостей, которые активно используются хакерами по всему миру.

 Каждая уязвимость, добавленная в этот каталог, должна быть устранена всеми федеральными гражданскими агентствами США в течение трех недель. Этот инструмент создан для обеспечения оперативного реагирования на реальные угрозы и своевременного устранения уязвимостей, прежде чем они будут эксплуатироваться нарушителями." data-html="true" data-original-title="KEV" >KEV также добавлен недавно обнаруженный недостаток, влияющий на продукты безопасности сетевых шлюзов Check Point (CVE-2024-24919 с оценкой CVSS 3.1: 7,5). Данная уязвимость позволяет атакующему читать определенную информацию на подключенных к Интернету шлюзах с включенным удаленным доступом VPN или мобильным доступом. Зафиксированные попытки атак в основном направлены на удаленные сценарии доступа через старые локальные аккаунты с нерекомендуемой аутентификацией по паролю.

Ввиду активной эксплуатации CVE-2024-1086 и CVE-2024-24919 федеральным агентствам рекомендуется применить последние исправления до 20 июня 2024 года, чтобы защитить свои сети от потенциальных угроз.