CISA и NIST теряют хватку, но частный сектор спасает положение.

В мае 2024 года компания Компания VulnCheck – это провайдер решений для управления кибербезопасностью, специализирующийся на автоматическом обнаружении уязвимостей в информационных системах организаций.

 Компания предлагает инструменты для сканирования и анализа безопасности веб-приложений, сетевых устройств и серверов, а также обеспечивает контроль соответствия стандартам безопасности и обнаружение утечек конфиденциальных данных.

 VulnCheck также предоставляет отчёты о найденных уязвимостях, оценку рисков и рекомендации по исправлению проблем безопасности. Компания работает со многими организациями, в том числе финансовыми учреждениями, телекоммуникационными компаниями и правительственными органами." data-html="true" data-original-title="VulnCheck" >VulnCheck зафиксировала 103 уязвимости (CVE), которые были впервые публично раскрыты как эксплуатируемые. По сравнению с апрелем это количество возросло на 90,7%, что соответствует общему росту числа эксплуатируемых уязвимостей. Тем временем, в отчёте Verizon за 2024 год говорится о 180% росте числа случаев эксплуатации уязвимостей с 2022 по 2023 год.

Из 103 уязвимостей с существующими доказательствами эксплуатации, выявленных в мае, 58 поставщиков программного обеспечения были связаны с 73 уникальными продуктами. Среди них лидируют Google Chrome (7 уязвимостей), Microsoft Windows (5), Apple Safari (5) и Adobe Acrobat Reader (3). Также выделяются Microsoft Exchange, Oracle JDK и phpMyAdmin с двумя уязвимостями каждая. Новичками в списке стали TP-Link TL-R600VPN и Arcserve Unified Data Protection.

Значительное увеличение раскрытия информации о новых эксплуатациях уязвимостей связано с несколькими факторами. Среди них — публикации отчётов Fortinet, CheckPoint и Aqua Security, которые предоставили данные о 49 уникальных уязвимостях. Это свидетельствует о готовности вендоров делиться более широкими сведениями об эксплуатациях, что является положительным трендом для команд по безопасности.

Сама компания VulnCheck также отмечает значительное снижение производительности таких мастодонтов в мире ИБ, как 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 и NIST – это Национальный институт стандартов и технологий, подразделение Министерства торговли США. Ранее известный как Национальное бюро стандартов, NIST продвигает и поддерживает стандарты измерений. У него также есть активные программы для поощрения и помощи промышленности и науки в разработке и использовании этих стандартов." data-html="true" data-original-title="NIST" >NIST. Так, в мае CISA добавила лишь 14 активно эксплуатируемых уязвимостей в свой список 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, что составляет 13,6% от числа таких же уязвимостей, обнаруженных VulnCheck за этот период.

Тем временем, NIST добавила в свою базу Национальная база данных уязвимостей (National Vulnerability Database, NVD) — это американский интернет-ресурс, который собирает, анализирует и распространяет информацию о проблемах безопасности в программном обеспечении, аппаратных устройствах и других технологических продуктах.

 NVD является частью Национального института стандартов и технологий США (NIST) и предоставляет информацию о характеристиках уязвимостей, их уровнях опасности, доступных исправлениях и рекомендациях по устранению проблем. Этот ресурс помогает организациям эффективно управлять киберрисками и обеспечивать безопасность своих информационных систем." data-html="true" data-original-title="NVD" >NVD лишь 22 из 103 уязвимостей, зафиксированных VulnCheck. И даже из этих 22 уязвимостей, 10 всё ещё ожидали анализа на конец мая.

В сфере американской кибербезопасности, которая часто являлась мировым примером в организации и подсчёте уязвимостей, прямо на наших глазах сейчас происходит значительное смещение сил. Частные компании выходят на передний план, демонстрируя значительный отрыв от государственных органов в области обнаружения и информирования об эксплуатируемых уязвимостях.

Эти коммерческие игроки демонстрируют более высокую эффективность и готовность

делиться актуальными данными, в то время как традиционные лидеры, такие как CISA и NIST, существенно отстают в своей способности отслеживать и своевременно сообщать об угрозах.

Этот сдвиг свидетельствует о растущей роли частного сектора в обеспечении кибербезопасности и необходимости тесного сотрудничества между коммерческими и государственными структурами для эффективного противостояния постоянно меняющимся киберугрозам.