Как NIST планирует вернуть прежние темпы работы с ошибками.

Национальный институт стандартов и технологий (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) объявил о заключении нового контракта с внешним подрядчиком, который поможет федеральному правительству в обработке программных и аппаратных уязвимостей из базы 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.

В последние месяцы официальные лица правительства, эксперты по кибербезопасности и ИБ-специалисты неоднократно выражали обеспокоенность по поводу накопившегося объема новых уязвимостей, которые не были проанализированы или дополнены с февраля, когда агентство объявило о сокращениях. Дополнение включает добавление контекстных данных к описанию уязвимости.

Представитель NIST сообщил, что новый контракт предусматривает предоставление «дополнительной поддержки в обработке поступающих CVE», которые будут добавлены в NVD. В NIST уверены, что дополнительная поддержка позволит в течение ближайших нескольких месяцев вернуться к темпам обработки, которые институт поддерживал до февраля 2024 года. Агентство работает с 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 над добавлением необработанных CVE в базу данных.

NIST рассчитывает, что накопившийся объем будет устранен к концу финансового года, который завершится 30 сентября. Однако представитель NIST не стал отвечать на вопросы о том, какая компания была нанята для помощи в обработке уязвимостей и насколько дешевле для правительства поручать такие задачи сторонним организациям.

В NIST работают над решением проблемы «увеличивающегося объема уязвимостей с помощью обновлений технологий и процессов». Цель агентства — создать программу, которая будет устойчивой в долгосрочной перспективе и поддерживать автоматизацию управления уязвимостями, измерения безопасности и соответствия требованиям.

NIST заверил, что «полностью привержен поддержке и модернизации ресурса, который жизненно важен для построения и поддержания доверия к информационным технологиям и стимулирования инноваций». Агентство планирует предоставлять дальнейшие обновления по мере попыток возвращения к нормальному уровню операционной деятельности.

С момента создания в 2005 году NVD стала незаменимым ресурсом для экспертов и ИБ-специалистов. В апреле NIST объяснил задержки в анализе уязвимостей увеличением объема программного обеспечения и изменениями в поддержке межведомственных программ. На сайте агентства было размещено уведомление о том, что оно «работает над созданием консорциума для решения проблем в программе NVD и разработки улучшенных инструментов и методов».

NIST недавно пришлось сократить бюджет на текущий финансовый год на 12% по сравнению с предыдущим годом. Ранее в NVD отмечали, что штат сотрудников NVD остался неизменным — 21 человек, в то время как количество поступающих уязвимостей продолжает расти.

Исследователи из VulnCheck проанализировали активность NVD с момента объявления сокращений 12 февраля и обнаружили, что из 12 720 новых уязвимостей 11 885 не были проанализированы или дополнены важными данными, которые помогают ИБ-специалистам определить, какое ПО было затронуто уязвимостью.

Анализ VulnCheck

8 мая агентство CISA объявило о запуске программы Vulnrichment для добавления метаданных к уязвимостям. MITRE, управляющая программой CVE, также утвердила

новые правила для организаций, присваивающих CVE. Десятки экспертов по кибербезопасности ранее подписали письмо, адресованное Конгрессу и министру торговли США Джине Раймондо, призывая их финансировать и защищать NVD, называя её «критически важной инфраструктурой для множества продуктов кибербезопасности».