Вей ТАЙ
старший научный сотрудник
по анализу данных Tenable

Илья ОСАДЧИЙ
директор по развитию
ООО «Тайгер Оптикс»

Никита ЦЫГАНКОВ
руководитель направления
внедрения средств защиты
информации АО «ДиалогНаука»

РЕЙТИНГ ОСОБОГО НАЗНАЧЕНИЯ

КАК КИБЕРРАЗВЕДКА И BIG DATA ПОМОГАЮТ ОЦЕНИВАТЬ КРИТИЧНОСТЬ УЯЗВИМОСТЕЙ И ПРИОРИТИЗИРОВАТЬ ИХ УСТРАНЕНИЕ

В статье рассматривается подход компании Tenable к оценке критичности вновь публикуемых уязвимостей до публикации CVE и метрик CVSS, а также подходы к изменению критичности уязвимостей в зависимости от изменения ландшафта угроз и активности злоумышленников.

Исследования аналитиков компании Tenable, разработчика решений по управлению уязвимостями, показывают, что злоумышленники зачастую используют уязвимости сразу же после их публичного раскрытия. В случае угроз нулевого дня уязвимости используются ещё до того, как о них становится известно широкому кругу специалистов. В этой статье мы рассмотрим, как VPR, или рейтинг приоритетности уязвимости, уникальная разработка Tenable, может использоваться для приоритизации устранения уязвимостей ещё до их официальной публикации в реестре National Vulnerability Database (NVD).

ОТ ОБНАРУЖЕНИЯ УЯЗВИМОСТИ ДО ПУБЛИКАЦИИ CVE ID

NVD — это репозиторий уязвимостей, состоящий из множества наборов данных, одним из которых является Common Vulnerabilities and Exposures (общеизвестные уязвимости, CVE). NVD является одним из основных источников информации об уязвимостях для исследователей и специалистов по информационной безопасности. Информация об уязвимости в базе NVD включает её идентификатор CVE ID, описание, сведения о затронутых платформах, метрики CVSS (v2 и v3) и другие данные. Обычно организация, сообщающая об уязвимости (так называемая CNA), присваивает ей идентификатор CVE ID сразу же при обнаружении. Затем CNA начинает подготовку описания уязвимости для публикации в NVD, в том числе результаты анализа влияния уязвимости на защищённость. Готовое описание CVE отправляется для публикации в базе NVD.

ЧТО ТАКОЕ «ПЕРИОД ДО NVD»

Процесс публикации CVE, описанный выше, может привести к задержке между первоначальным публичным раскрытием уязвимости и её публикацией в NVD. NVD подтверждает существование такой задержки и указывает на следующее: «Дата 'Date Entry Created' в записи CVE указывает на день, когда идентификатор CVE ID был присвоен CVE Numbering Authority (CNA) или запись CVE была опубликована в реестре CVE. Эта дата не указывает на то, когда уязвимость была обнаружена, когда о ней сообщили вендору, когда она была публично обнародована или была обновлена в CVE».

В качестве примера «периода до NVD» рассмотрим уязвимость CVE-2019–17026. Изначально она была опубликована в Mozilla Security Advisory 8 января 2020 года, в NVD появилась 2 марта 2020 года и два дня спустя получила метрики CVSS. В данном примере «период до NVD» длился с 8 января до 2 марта и составил целых 55 дней.

СЕРЬЁЗНОСТЬ ПРОБЛЕМЫ «ПЕРИОДА ДО NVD»

Промежуток до NVD не является редкостью — 71 000 CVE были раскрыты в бюллетенях вендоров до того, как были опубликованы в NVD, что составляет половину всех CVE. В 2019 году у 5 300 CVE наблюдалось наличие периода до NVD.

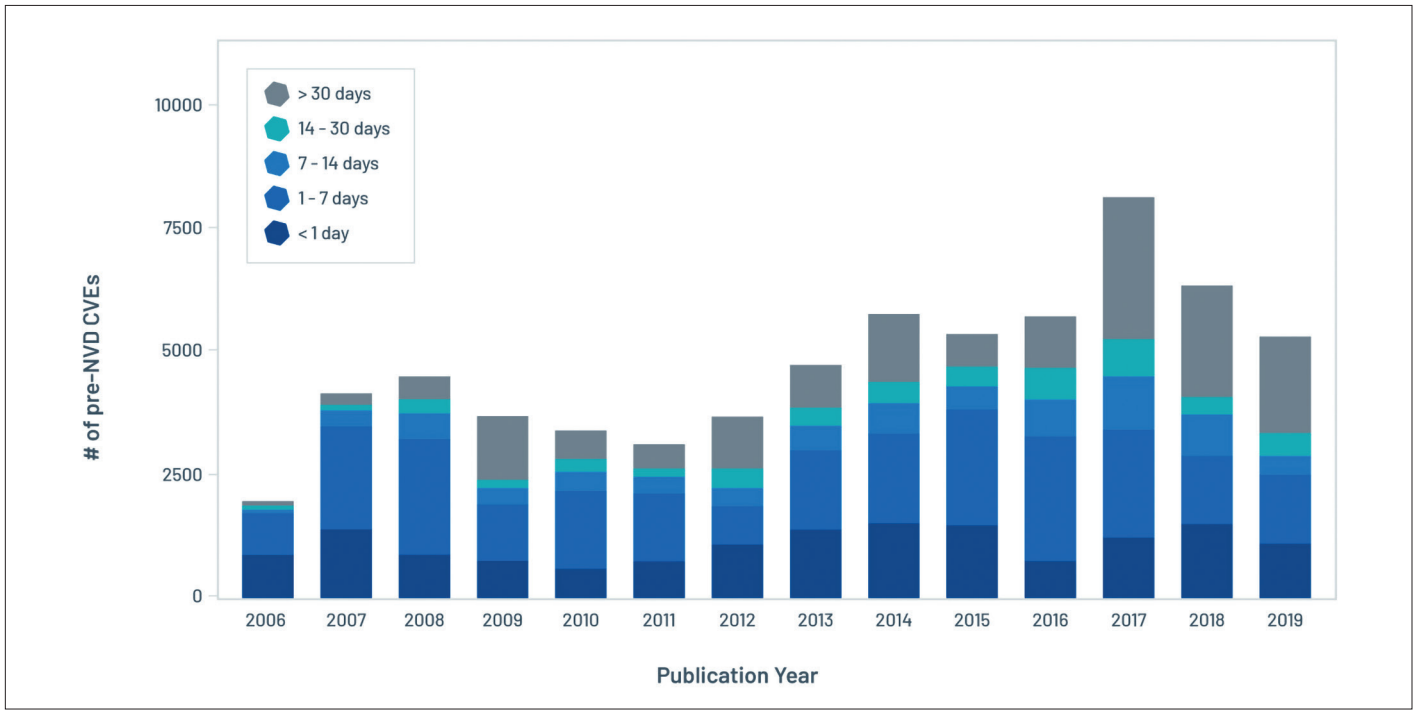

Рисунок 1. Количество CVE с периодом до NVD с 2006 года

В то время как «период до NVD» для некоторых CVE составляет один день, что приемлемо, анализ, проведённый Tenable, показывает, что для многих уязвимостей задержка существенна. На рисунке 1 приведено количество CVE с периодом до NVD с 2006 года, с разбивкой по годам и длительности задержки в публикации.

Из этого графика можно сделать следующие выводы:

- Начиная с 2013 года ежегодное количество CVE с «периодом до NVD» стабилизировалось на показателе в 5 000 единиц. Это означает, что в последние годы CNA стали более оперативно публиковать CVE.
- В последние годы стало более выраженным распределение длительностей задержки в публикации уязвимости. Значительная часть уязвимостей была опубликована с задержкой в 30 и более дней. Специалисты ИБ должны уделять внимание CVE со значительным периодом до NVD, поскольку такие уязвимости могут отрицательным образом сказаться на защищённости организаций.

АКТИВНОСТЬ ЗЛОУМЫШЛЕННИКОВ ДО ПУБЛИКАЦИИ В NVD

Очевидно, что злоумышленники не ждут публикации CVE для начала активной эксплуатации уязвимости. Сравнение данных киберразведки со списком CVE с «периодом до NVD» показывает, что в отношении 5 400 из 43 000 CVE (12%), опубликованных с 2019 по 2020 год, наблюдалась активность злоумышленников ещё до публикации данных в NVD.

На рисунке 2 отражено распределение этих CVE по году публикации и «окну угрозы» до публикации в NVD. Значительное количество этих CVE активно использовалось злоумышленниками в течение как минимум 30 дней до их публикации в NVD. Поэтому любые системы, затронутые этими уязвимостями, оставались подвержены реальным атакам до того, как информация об уязвимости стала доступна в NVD.

КАК ПРИОРИТИЗИРОВАТЬ УСТРАНЕНИЕ УЯЗВИМОСТЕЙ ДО NVD С ПОМОЩЬЮ РЕЙТИНГА VPR

Устранение активно эксплуатируемых уязвимостей необходимо начинать как можно раньше. Как показало исследование, CVE из реестра NVD не являются наиболее актуальным источником информации для организации проактивного управления уязвимостями. Tenable решает эту проблему, получая информацию об уязвимостях напрямую из бюллетеней более чем от 100 крупнейших вендоров. Для полученных таким образом уязвимостей Tenable рассчитывает рейтинг приоритетности уязвимости, или VPR.

Расчёт VPR для уязвимостей в «периоде до NVD» не является тривиальной задачей. Поскольку многие CNA не предоставляют метрики CVSS для уязвимости на стадии до NVD, оценка влияния уязвимости на их основе не всегда возможна. Для решения этой проблемы VPR комбинирует технологии машинного обучения и обработки натурального языка, что позволяет предсказать метрики CVSS.

Начиная с августа 2019 года Tenable проводит оценку критичности уязвимостей до их публикации в NVD с помощью модели VPR. Из 12 073 опубликованных уязвимостей 1 592 включали «период до NVD». По итогам анализа рейтинг VPR показал гораздо большую эффективность в оценке новых уязвимостей. Например:

- все 1 592 уязвимости получили рейтинг VPR до публикации в NVD;
- 84% уязвимостей с «периодом до NVD» получили рейтинг VPR в течение уже первых 24 часов, в то время как только 38% уязвимостей были опубликованы в NVD в тот же период;

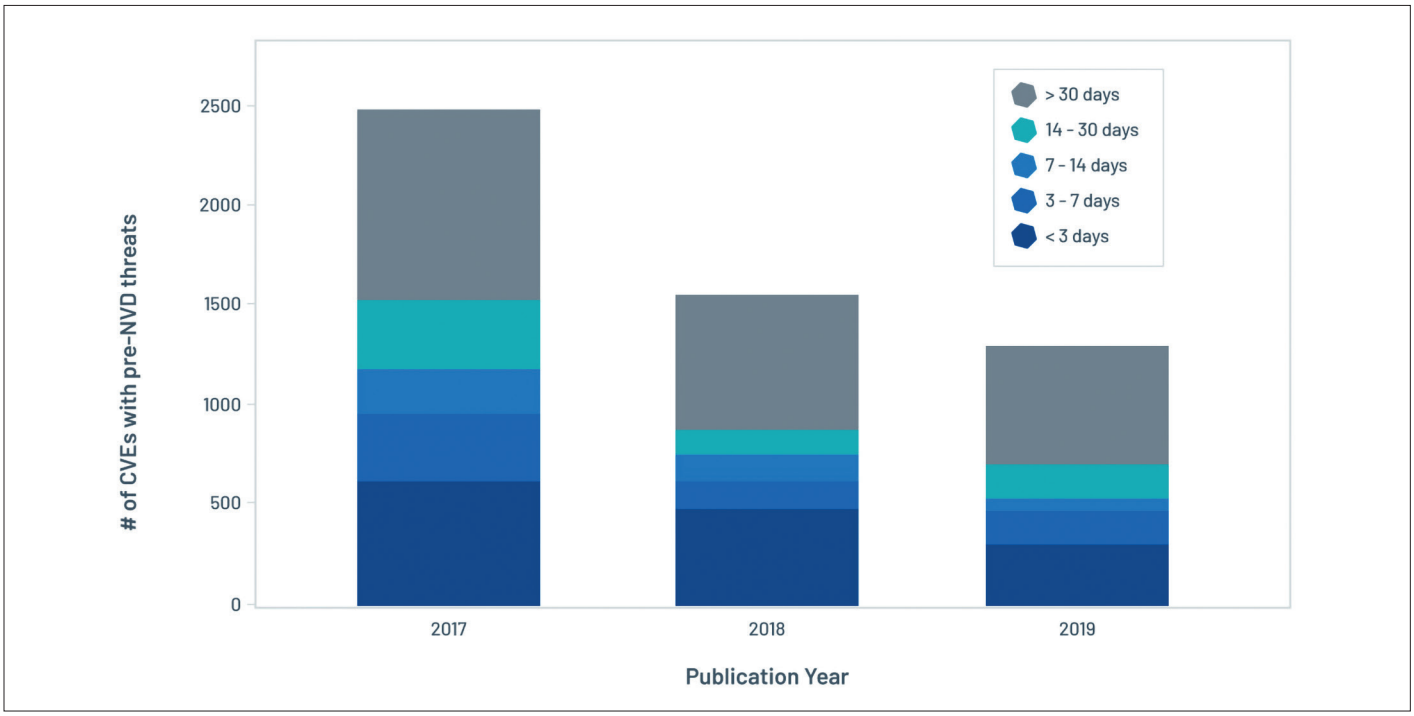

Рисунок 2. Количество CVE с активными угрозами до публикации в NVD. Разбивка по длительности «окна угрозы»

◆ 499 уязвимостей были опубликованы в NVD с задержкой в семь или более дней, в то время как только 101 уязвимости были присвоены рейтинги VPR за семь и более дней;

◆ 245 уязвимостей были опубликованы в NVD с задержкой более 30 дней.

Количество уязвимостей с «периодом до VPR» будет уменьшаться и далее по мере того, как Tenable будет получать данные об уязвимостях из всё большего числа бюллетеней вендоров.

ПРАКТИЧЕСКИЙ ПРИМЕР: CVE-2019–17026

В качестве примера в этой статье используется CVE-2019–17026. Вот как развивались события с этой уязвимостью:

◆ **8 января 2020 года:** CVE-2019–17026 был впервые опубликован в бюллетене Mozilla Security Advisory. Tenable опубликовал анализ уязвимости после её публикации и плагины, позволяющие её детектировать. Они были опубликованы с рейтингом VPR 9,7, что отразило факт использования уязвимостей в нацеленных атаках.

◆ **Период с 8 января по 1 марта 2020 года**: дискуссии и исследования об эксплуатации этой уязвимости были зафиксированы во многих источниках, в том числе в Twitter, форумах злоумышленников, сайтах Dark Web и в технических блогах. Это привело к повышению рейтинга VPR до пикового значения 9,9 на этапе до публикации в NVD;

◆ **2 марта 2020 года:** CVE-2019–17026 был опубликован в NVD, и два дня спустя в результате анализа уязвимость получила оценку CVSSv3 8,8;

◆ **3 марта 2020 года и позже:** риск, связанный с этой уязвимостью, остаётся высоким. События, связанные с ней, были зафиксированы в прессе, Twitter, сайтах Dark Web, на пейст-сайтах и т.д. В апреле появилась информация о том, что эта уязвимость использовалась APT-злоумышленником по имени DarkHotel для целей в Китае и Японии. Рейтинг VPR этой уязвимости остаётся критическим на момент публикации.

ВЫВОДЫ

В этой статье мы показали, что злоумышленники зачастую используют уязвимости ещё до публикации соответствующих CVE в реестре NVD. Учитывая имеющиеся задержки в публикации, специалисты ИБ не должны использовать NVD как единственный источник информации об уязвимостях. Рейтинг VPR, разработанный Tenable, оперативно оценивает новые уязвимости — 84% новых уязвимостей оцениваются алгоритмом VPR в течение одного дня с момента публичного раскрытия, и 93% оцениваются в течение одной недели.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

◆ опробовать VPR в действии можно, заказав пилот решений Tenable.io (в облаке) и Tenable.sc (на площадке заказчика): *https://www.tiger-optics.ru/get-demo/*

◆ узнать больше о предсказательной приоритизации Tenable и рейтинге VPR можно по ссылке Tenable Predictive Prioritization and VPR: *https://www.tenable.com/tenable-io/predictive-prioritization-demo*