Список использованных источников:
1.Хортон, У. Электронное обучение: инструменты и технологии. Пер. с англ. / У. Хортон, К.. Хортон. – М.: КУДИЦ–ОБРАЗ, 2005. 640 с.

ИССЛЕДОВАНИЕ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-СЕРВЕРА VCENTER SERVER 5.5

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Поклонский С.А., Прузан А.Н.

Охрименко А. А. – канд. техн. наук, доцент

Рассматриваются вопросы достаточности работ по тестированию информационной безопасности программного обеспечения веб-сервера vCenter Server 5.5. Показывается, что качество и объём таких работ недостаточны для полного устранения дефектов программного обеспечения сервера.

Под угрозой информационной безопасности информационного объекта принято понимать возможные воздействия на него, приводящие к ущербу. Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, называется уязвимостью. В докладе на примере веб-сервера vCenter Server делается попытка исследования результатов тестирования информационной безопасности таких сложных информационных объектов, как веб-сервера.

Под веб-сервером обычно понимают сервер, принимающий HTTP-запросы от клиентов (обычно веб-браузеров) и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными. Веб-сервером называют как ПО, выполняющее функции веб-сервера, так и непосредственно компьютер, на котором установлено это ПО.

В последнее время, когда в ИТ-индустрии стали широко использоваться облачные технологии [1, 2], для реализации последних очень популярной стала серверная виртуализация. Одним из главных компонентов серверной виртуализации, предложенной американской компанией VMware, является VMware vSphere – платформа для виртуализации ИТ-инфраструктуры предприятия. Платформа vSphere подразумевает одновременное использование ESXi хостов (x86) и vCenter Server для их централизованного управления.

vCenter Server – главный инструмент управления для администраторов vSphere. Он предоставляет единую точку контроля за всеми компонентами в виртуальном датацентре и выполняет некоторые важные функции. vCenter позволяет конфигурировать новые ESXi хосты, хранилище (в т. ч. облачное [1, 2]), сеть и характеристики виртуального оборудования различных инфраструктурных компонентов, создавать и импортировать новые виртуальные машины, производить мониторинг и отчёты о производительности гостевой ОС, виртуальных машин и ESXi хостов. vCenter управляет правами, разрешениями, ролями на различных уровнях виртуальной инфраструктуры, унифицирует ресурсы различных хостов ESXi и позволяет обеспечивать общий доступ к ним для любых виртуальных машин в датацентре. Это достигается назначением ресурсов кластера хостов ESXi виртуальным машинам с учётом назначенных администратором политик.

При разработке программного обеспечения веб-серверов и веб-приложений широко используется такой вид нефункционального тестирования как тестирование безопасности. При этом применяются такие вспомогательные очень сложные программные средства, как Wapiti 2.1.0, Netsparker Community Edition, N-Stalker Free Version, Websecurify, Skipfish, OWASP WebScarab Project и другие.

Тем не менее, проведенное тестирование не всегда помогает полностью выявить уязвимости веб-сервера. Пример: 29 декабря 2016 года американским институтом NIST была выявлена и внесена в базу уязвимостей новая уязвимость CVE-2016-7460 сервера vCenter Server 5.5. Уязвимость была обнаружена в одной из функций ПО сервера – функции Single Sign-On. Уязвимость позволяла удаленным злоумышленникам читать произвольные файлы или вызывать отказ в обслуживании через XML-документ содержащий объявление внешней сущности, связанной с ссылкой на сущность, относящуюся к XML External Entity (XXE) уязвимости. На стадии тестирования безопасности сервера уязвимость не удалось обнаружить, и только к 01.03.2017 компании VMware удалось устранить присутствующие в ПО сервера дефекты. Компания при этом понесла как материальные (известно, что цена устранения дефекта тем меньше, чем раньше он обнаружен), так и моральные (потеря репутации у потребителей) убытки.

Вывод: Тестированию безопасности на стадии разработки ПО серверов уделяется недостаточно внимания. Объём работ по тестированию безопасности надо увеличить, а их качество – повысить.

Список использованных источников:
1. Прузан А.Н. Мониторинг инцидентов информационной безопасности в облачных вычислениях на малом предприятии/ Прузан А.Н., Николаенко В. Л., Сечко Г. В. // Доклады БГУИР. – 2015 – № 7 (93). – С. 126–128.
2. Николаенко, В.Л. Опыт мониторинга инцидентов информационной безопасности в облачных вычислениях/ В.Л. Николаенко, А.Н. Прузан, Г.В.Сечко, Т.Г. Таболич // Сб. статей III межд. заоч. НПК «Информационные системы и технологии: управление и безопасность» (декабрь 2014). – Тольятти- 2014. – 345 с. – С. 209–215