Функциональные возможности программного обеспечения «Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)»

ООО «Сивиэй Технолоджиес»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)»

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

На 6 листах

Ростов-на-Дону
2023

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки товарные знаки принадлежат их владельцам.

Товарные знаки «NeuroFortress», «NF WAF», «NF Web Application Firewall», принадлежат ООО «Сивиэй Технолоджиес», «CVA Technologies».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

.

СОДЕРЖАНИЕ

1. Общая информация

Программный продукт «Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)» - это совокупность программных мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение. NF Web Application Firewall (NF WAF) устанавливается перед защищаемым веб ресурсом и анализирует все передаваемые HTTP запросы на наличие вредоносного кода и потенциально опасную активность злоумышленников. При проведении анализа NF Web Application Firewall основывается на различных механизмах сигнатурного анализа, правилах, средствах анализа аномалий. Также в своей работе NF Web Application Firewall (NF WAF) могут использовать нейросети и различные индикаторы атак.

В случае обнаружения вредоносных запросов NF Web Application Firewall (NF WAF)может выполнить следующие действия: удалить из запроса опасные данные по аналогии с тем, как антивирус пытается лечить зараженные файлы, также запрос может быть заблокирован целиком. Также возможна блокировка источника атаки на сетевом уровне, то есть, блокировка всех обращений с данного IP-адреса.

2. Функциональные характеристики ПО NF Web Application Firewall (NF WAF)

Механизмы фильтрации NF Web Application Firewall (NF WAF) позволяют противодействовать следующим типам вредоносной активности в отношении веб-приложений:

• Межсайтовый скриптинг (XSS).

• Удаленное выполнение произвольного кода (RCE).

• SQL-, NoSQL-инъекции.

• Подбор учетных данных (Brute-force).

• XML External Entities (XXE).

• Удаленное выполнение произвольного кода (RCE).

• Перехват сессий пользователя. • Кража личных данных пользователей.

- Мониторинг сети в режиме реального времени;

- Быстро реагировать на любые разновидности атак на веб-приложения;

Проверка и анализ контента, который создан при помощи HTML и DHTML, а также CSS и прикладных протоколов передачи HTTPS, HTTP;

- Предотвращение утечки информации, проверяя исходящий от веб-приложений трафик HTTP/HTTPS, и принимая заданные меры на основании заданных активных правил;

- Постоянное формирование журнала событий;

- регистрация событий (атак);

- отображение исчерпывающей информации об атакующем IP-адресе;

- Защищать от атак, направленных конкретно на сам NF Web Application Firewall (NF WAF);

- отображение исчерпывающей информации о сервисе, который подвергся атаке со стороны злоумышленников;

- возможность заблокировать атакующий IP-адрес;

- создание правил реагирования на события;

- добавление IP-адреса в список исключений;

- добавление URL-адреса в список исключений.