Дата обновления документа: 21.05.2024

Рекомендации по обеспечению безопасности применения ПК «С-Терра СОВ» версии 4.3 в условиях наличия уязвимостей прикладного и системного ПО

Рекомендации по обеспечению безопасности

Для обеспечения безопасности применения ПК «С-Терра СОВ» версии 4.3 в условиях наличия уязвимостей прикладного и системного ПО следует выполнять следующие требования.

1. Рекомендуется произвести в Продукте следующие настройки:

   В "Веб-интерфейс" - "Настройки" - "Шаблоны" - Шаблоны с путём "/etc/suricata/suricata.yaml" в разделе "app-layer" - "protocols" изменить секции

   ```
   http2:
         enabled: yes
   http:
         enabled: yes
   snmp:
         enabled: yes
   ```

   на

   ```
   http2:
         enabled: no
   http:
         enabled: no
   snmp:
         enabled: no
   ```

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2024-23836, CVE-2024-23837.

Для снижения влияния данных уязвимостей следует:

- В разделе "Веб-интерфейс" - "Настройки" - "Шаблоны" - Шаблоны с путём "/etc/suricata/suricata.yaml" уменьшить параметр `stream.reassembly.depth`;
- В разделе "Веб-интерфейс" - "Правила" - "Список правил" воспользоваться поиском правил с содержимым `http.request_header` и `http.response_header keywords` и выключить/изменить их на усмотрение администратора.

Отдельные уязвимости, отсутствие которых проверено

1. Уязвимость *CVE-2024-23839* не применима к Продукту: отсутствует уязвимый код.