Дата обновления документа: 29.10.2025

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.

2. Рекомендуется в Продукте исключить использование следующих преобразований file.data в БРП для ПО Suricata:
   - to_lowercase;
   - to_uppercase;
   - strip_whitespace;
   - compress_whitespace;
   - dotprefix;
   - header_lowercase;
   - strip_pseudo_headers;
   - url_decode;
   - xor.

   Данная мера позволяет нейтрализовать следующие уязвимости:
   CVE-2024-55605 (БДУ 2025-00134).

3. Рекомендуется в Продукте не выполнять команду `suricata -F` по отношению к файлам, полученным из недоверенных источников.

   Данная мера позволяет нейтрализовать следующие уязвимости:
   CVE-2024-55626 (БДУ 2024-11374).

4. Рекомендуется в Продукте отключить в ПО Suricata обработку протокола DNS, для этого администратору нужно выполнить в панели администратора действия:
   на вкладке Настройки - Шаблоны найти пункт "Конфигурационный_файл_Suricata", открыть его на редактирование. Найти строки по пути "app-layer: -> protocols: -> dns -> tcp -> enabled", а также "app-layer: -> protocols: -> dns -> udp -> enabled". Установить их значение в no так, чтобы получилось:

```
app-layer:
  protocols:
    dns:
      tcp:
        enabled: no
        detection-ports:
          dp: 53
      udp:
        enabled: no
        detection-ports:
          dp: 53
```

   Применить изменения на вкладке "Узлы" - "Применить изменения для всех узлов".

   Данная мера позволяет нейтрализовать следующие уязвимости:
   CVE-2024-55628 (БДУ 2025-00136).

5. Рекомендуется в Продукте средствами межсетевого экрана заблокировать TCP пакеты с флагом URG (примечание - данная фильтрация может приводить к неработоспособности некоторых FTP подключений).

   Данная мера позволяет нейтрализовать следующие уязвимости:
   CVE-2024-55629 (БДУ 2025-00137).

6. Рекомендуется в Продукте добавить следующие правила в настройки для выявления попыток эксплуатации уязвимости:

```
alert tcp any any -> any any (msg:"Multiple SYN packets from same src";
flags:S; threshold: type both, track by_src, count 5, seconds 10;
sid:1001101; rev:1;)

alert tcp any any -> any any (msg:"Rapid SYN sequence"; flags:S;
threshold: type threshold, track by_src, count 10, seconds 1; sid:1001102;
rev:1;)

alert tcp any any -> any any (msg:"SYN on established connection";
flow:established; flags:S; sid:1001103; rev:1;)
```

Администратору безопасности рекомендуется регулярно анализировать журналы событий и при выявлении массовых попыток эксплуатации принимать меры по блокированию источника атак.
Кроме того, для усиления безопасности сетевой инфраструктуры рекомендуется использовать следующие настройки для межсетевого экрана, установленного до СЗИ (приводятся в синтаксических правилах известного ПО iptables):

```
sudo iptables -A FORWARD -p tcp --syn -m hashlimit --hashlimit-name
synflood --hashlimit-mode srcip,srcport,dstip,dstport --hashlimit-above
1/sec -j DROP
```

Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2025-59147 (БДУ 2025–12460).

Отдельные уязвимости, отсутствие которых проверено

1. Уязвимость *CVE-2024-23839* не применима к Продукту: отсутствует уязвимый код.
2. Уязвимость *CVE-2024-55627 (БДУ 2025 – 00135)* не применима к Продукту: уязвимый код отсутствует в Продукте. Уязвимость привнесена в более поздней версии ПО Suricata.