I. Рекомендации по устранению уязвимостей операционной системеFortiOS

1. Уязвимость SSL VPN веб-портала операционной системы FortiOS (BDU:2022-02981, уровень опасности по CVSS 2.0 – высокий уровень опасности, по CVSS 3.0 – высокий уровень опасности), существующая из-за неверного ограничения имени пути к каталогу с ограниченным доступом. Эксплуатация данной уязвимости может позволить нарушителю, действующему удаленно, получить доступ к системным файлам путем специально сформированного HTTP-запроса.

В случае невозможности установки обновления программного обеспечения (далее - ПО) необходимо принять следующие меры:

- полностью отключить службу IPSEC-VPN и SSL-VPN (как в веб-режиме, так и в туннельном режиме);
- выполнить смену пароля для всех учетных записей;
- включить многофакторную аутентификацию.

2. Уязвимость операционной системы FortiOS (BDU:2022-04724, уровень опасности по CVSS 2.0 – критический уровень опасности, по CVSS 3.0 – критический уровень опасности), связанная с недостатками процедуры аутентификации. Эксплуатация данной уязвимости может позволить нарушителю, действующему удаленно, войти в систему без запроса второго фактора аутентификации (FortiToken).

В случае невозможности установки обновления ПО необходимо принять следующие меры:

- использовать аутентификацию через протокол LDAP только для пользователей, не использующих двухфакторную аутентификацию;
- для пользователей, использующих двухфакторную аутентификацию, удалить одноименные записи в службе каталогов LDAP или выделить их в отдельную группу, не используемую в FortiGate.

При невозможности выполнения указанных мер рекомендуется использовать FortiAuthenticator или отключить аутентификацию через протокол LDAP.

3. Уязвимость операционной системы FortiOS (BDU:2019-04699, уровень опасности по CVSS 2.0 - низкий уровень опасности, по CVSS 3.0 - низкий уровень опасности), связанная с ошибками авторизации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить несанкционированный доступ к защищаемой информации, выдавая себя за LDAP- сервер.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

- для пользователей, использующих FortiOS версии с 6.0.3 по 6.2.0, включить параметр CLI, который проверяет подлинность LDAP-сервера. Этот параметр можно включить только в том случае, если установлены параметры secure и ca-cert LDAP-сервера;

- для пользователей, использующих FortiOS версии с 6.0.2 и ниже, отключить аутентификацию LDAP.

4.Уязвимость веб-интерфейса управления операционных систем FortiOS и прокси-сервера для защиты от интернет-атак FortiProxy (BDU:2022-06189, уровень опасности по CVSS 2.0 – критический уровень опасности, по CVSS 3.0 – критический уровень опасности), связанной с возможностью обхода аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие меры:

-использовать локальную политику для ограничения доступа к веб-интерфейсу управления;

-отключить возможность доступа к веб-интерфейсу управления из общедоступных сетей (Интернет);

-ограничить возможность подключения к веб-интерфейсу, осуществлять подключение только с доверенных хостов.

II. Рекомендации по устранению уязвимостей операционной системеPAN-OS

1. Устранения уязвимости веб-интерфейса операционной системы PAN-OS централизованной системы управления межсетевыми экранами Palo Alto Networks Panorama (BDU:2022-06333, уровень опасности по CVSS 2.0 — высокий уровень опасности, по CVSS 3.0 — высокий уровень опасности), связанная с возможность обхода аутентификации. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

-ограничить использование программного средства из-за отсутствия поддержки производителем;

-использовать средства межсетевого экранирования с целью ограничения доступа к веб-интерфейсу программного средства;

-ограничить доступ к веб-интерфейсу программного средства путем внедрения механизма «белого» списка IP-адресов.

III. Рекомендации по устранению уязвимостей операционной системе JunOS

1.Устранения уязвимости файла jrest.php веб-интерфейса операционной системы JunOS (BDU:2022-06608, уровень опасности по CVSS 2.0 — высокий уровень опасности, по CVSS 3.0 — высокий уровень опасности), связанная с возможностью включения локальных PHP-файлов. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

-отключить веб-интерфейс J-Web;

-отключить доступ к веб-интерфейсу путем внедрения механизма «белого» списка IP-адресов.

IV. Рекомендации по устранению уязвимостей операционной системе JunOS

1. Уязвимость функции pr_pack() утилиты ping операционной системы FreeBSD (BDU:2022-07076, уровень опасности по CVSS 2.0 – критический уровень опасности, по CVSS 3.0 – критический уровень опасности), вызванная переполнением буфера в стеке при разборе ICMP-сообщений. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с root-привилегиями.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

-применить системы обнаружения и предотвращения вторжений для ограничения возможности обращения к уязвимой операционной системе и фильтрации трафика;

-ограничить возможность подключения к уязвимой операционной системе из общедоступной сети (Интернет);

-отключить возможность обработки ICMP-пакетов (ipfw add deny icmp from any to any).