Рекомендации органам государственной власти Республики Дагестан по устранению уязвимостей в иностранном программном обеспечении

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей иностранного программного обеспечения, необходимо устранить следующие уязвимости:

1. Уязвимость компонента Zabbix Frontend системы мониторинга Zabbix (BDU:2022-00884, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – критический) позволяет нарушителю обойти аутентификацию на серверах с настроенным языком разметки подтверждения безопасности SAML (открытый стандарт, обеспечивающий единую точку аутентификации (единый вход), которая обеспечивает обмен данными между поставщиком удостоверений и поставщиком услуг). В целях предотвращения возможности эксплуатации указанной уязвимости необходимо отключить аутентификацию SAML.

2. Уязвимость системы мониторинга Zabbix (BDU:2022-00876, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – средний), связанная с ошибками контроля доступа, которая позволяет злоумышленникам изменить файл конфигурации (скрипт setup.php) и получить доступ к панели управления с повышенными привилегиями. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо удалить setup.php файл.

3. Уязвимость операционной системы Cisco NX-JS (BDU:2022-01004, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – высокий) позволяет нарушителю, действующему удаленно, осуществлять команды от имени пользователя root. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо отключить функцию NX-API в настройках программного обеспечения Cisco NX-OS.

4. Уязвимость сетевого программного обеспечения Mozilla VPN (BDU:2022-00972, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – высокий) позволяет запускать произвольный код с привилегиями SYSTEM при использовании возможности загрузки файла конфигурации OpenSSL из

незащищенного каталога. В целях устранения указанной уязвимости необходимо исключить использование Mozilla VPN.

5. Уязвимость маршрутизаторов Huawei Engine (BDU:2022-00994, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий) позволяет нарушителю повысить свои привилегия в информационной системе. В целях устранения указанной уязвимости рекомендовано обновление до актуальной версии.

6. Уязвимость домена обработки потоков (flowd) операционной системы Juniper Networks Junos на устройствах серий MX и SRX (BDU:2022-00995, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий) позволяет нарушителю, действующему удаленно, вызвать сбой потока и тем самым реализовать атаку «отказ в обслуживании». В целях устранения указанной уязвимости необходимо отключить функции SIP ALG в настройках сетевого устройства.

7. Уязвимость модуля «vote» системы управления содержимым сайтов (CMS) 1С Битрикс (BDU:2022-01141, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – критический), связанная с возможностью отправки специально сформированных сетевых пакетов, позволяющая нарушителю, действующему удаленно, записать произвольные файлы в уязвимую систему. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- отключить или удалить модуль «vote»;

- осуществить настройку средств межсетевого экранирования прикладного уровня, позволяющую блокировать специально сформированные сетевые пакеты.

8. Уязвимость библиотеки cmark-gfm (BDU:2022-01140, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), позволяющая нарушителю, действующему удаленно, выполнить произвольный код. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- отключить расширения table extension;

- использовать входные данные для библиотеки только из доверенных источников.

9. Уязвимость программных продуктов Mozilla (BDU:2022-01146, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с

обращением к уже освобожденной области памяти (Use-after-free) в коде для обработки параметра XSLT, может позволить нарушителю, действующему удаленно, выполнить произвольный код. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- обеспечить доступ только к доверенным Интернет-ресурсам;

- осуществить настройку средств межсетевого экранирования прикладного уровня, позволяющую блокировать специально сформированные пакеты;

- осуществлять запуск браузера от имени пользователя с минимальными привилегиями.

10. Уязвимость программных продуктов Mozilla (BDU:2022-01147, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с обращением к уже освобожденной памяти IPC фреймворка WebGPU, может позволить нарушителю, действующему удаленно, выйти из изолированной программной среды. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- обеспечить доступ только к доверенным Интернет-ресурсам;

- осуществить настройку средств межсетевого экранирования прикладного уровня, позволяющую блокировать специально сформированные сетевые пакеты;

- осуществлять запуск браузера от имени пользователя с минимальными привилегиями.

11. Уязвимость API кластерной базы данных устройств Cisco Expressway Series и Cisco Telepresense VCS (BDU:2022-01148 уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с недостаточной проверкой введенных пользователем командных аргументов, может позволить нарушителю, действующему удаленно, перезаписать произвольные файлы на базовой операционной системе в качестве root-пользователя. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- ограничить доступ к API;

- организовать доступ к веб-интерфейсу только из определенного сегмента сети (сегментирование сети);

- осуществить настройку средств межсетевого экранирования прикладного уровня, позволяющую блокировать специально сформированные сетевые пакеты;

- использовать системы обнаружения и предотвращения вторжений.

12. Уязвимость веб-интерфейса управления устройствами Cisco Expressway Series и Cisco Telepresense VCS (BDU:2022-01149 уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с недостаточной проверкой введенных пользователем командных аргументов, может позволить нарушителю, действующему удаленно, выполнить произвольный код в качестве root-пользователя. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- ограничить доступ к веб-интерфейсу только из определенного сегмента сети (сегментирование сети);

- осуществить настройку средств межсетевого экранирования прикладного уровня, позволяющую блокировать специально сформированные сетевые пакеты;

- использовать системы обнаружения и предотвращения вторжений.

13. Уязвимость модуля разбора данных средств антивирусной защиты Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security, Kaspersky Small Office Security, Kaspersky Security Cloud, Kaspersky Endpoint Security (BDU:2022-01730, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), связанная с неограниченным распределением ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо обновить указанное программное обеспечение.

14. Уязвимость модуля средств антивирусной защиты Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security, Kaspersky Small Office Security, Kaspersky Security Cloud, Kaspersky Endpoint Security (BDU:2022-01729, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – средний), связанная с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю вызвать аварийное завершение работы операционной системы Microsoft Windows посредством запуска специально сформированного

приложения. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо обновить указанное программное обеспечение.

15. Кроме того, зарубежными хакерскими группировками активно эксплуатируются уязвимости в конфигурации серверов MS SQL Server. Компьютерные атаки начинаются со сканирования серверов открытых портов TCP 1433, после чего нарушители запускают специальное программное обеспечение для перебора паролей с целью вскрытия доступных паролей. С целью предотвращения доступа нарушителей к серверам MS SQL Server необходимо заблокировать их доступ к сети «Интернет», а также заблокировать доступ к серверам по порту TCP 1433.

Заблокировать возможность удаленного доступа иностранных подрядчиков (компаний) в локальные сети органов государственной власти, муниципальных органов и подведомственных им организаций, а также отключить автоматическое неконтролируемое обновление иностранного программного обеспечения.

16. Уязвимость веб-интерфейса управления системы балансировки трафика FortiWAN (BDU:2022-01972, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), связанной с непринятием мер по защите структуры SQL-запросов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с помощью специально сформированных HTTP-запросов. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо приять меры:

- ограничить доступ к веб-интерфейсу FortiWAN для внешних пользователей с использованием межсетевого экранирования;

- отключить доступ к веб-интерфейсу FortiWAN через WAN-интерфейсы;

- использовать межсетевой экран прикладного уровня или средства обнаружения вторжений.

При невозможности выполнения указанных мер рекомендуется отключить веб-интерфейс.

17. Уязвимость веб-сервера Atlassian Confluence Server и дата центра Confluence Data Center связана с ошибками при обработке входных данных

(BDU:2022-03284, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо приять меры:

-использование средств межсетевого экранирования уровня веб-приложений с целью ограничения доступа с URL-адресов, содержащих ${;

-ограничение доступа к веб-серверу из сети интернет;

-ограничение использования программного средства.

18. Уязвимость веб-интерфейса управления микропрограммного обеспечения маршрутизатора Cisco Small Business RV 110W, RV 130, RV 130W и RV 215W, связанная с недостаточной проверкой вводимых данных (BDU:2022-03519, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код или вызвать отказ в обслуживании путем отправки специально сформированных HTTP-пакетов.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

-выделение веб-интерфейса управления в отдельный сегмент сети с ограничением доступа к нему средствами межсетевого экранирования;

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

-использование межсетевого экрана уровня приложений;

-использование системы обнаружения и предотвращения вторжений.

19. Уязвимость функций внешней аутентификаций устройства управления защитой контента Cisco Secure Email and Web Manager (ранее Cisco Security Management Appliance и Cisco Email Security Appliance), связанная с ошибками разграничения доступа (BDU:2022-03520, уровень опасности по CVSS 2.0 –

критический, по CVSS 3.0 – критический). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к веб-интерфейсу устройства.

20. Устранение уязвимостей программного обеспечения для унификации и упрощения доступа к базам данных Spring Data MongoDB (BDU:2022-03714, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), связанной с ошибками при обработке SpEL-выражений. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированного SpEL-запроса.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

-использование символов «[0]» вместо «?0» при написании запроса;

-проверка параметров перед вызовами метода запроса;

-переконфигурирование BeanPostProcessor с ограничением QueryMethodEvaluationContextProvider.

21. Устранения уязвимости приложения сетевой файловой системы Samba (BDU:2022-04687, уровень опасности по CVSS 2.0 – высокий уровень опасности, по CVSS 3.0 – высокий уровень опасности), связанной с ошибками при проведении процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю изменить пароль произвольного пользователя и получить полный доступ к учетной записи.

В случае невозможности установки обновления данного ПО необходимо отключить поддержку протокола kpasswd, путем добавления в файл smb.conf строки «kpasswd port = 0».

22. Устранение уязвимости веб-сервера Atlassian Confluence Server и дата центра Confluence Data Center связана с ошибками при обработке входных данных (BDU:2022-04612, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанной с возможностью использования жестко закодированных

учетных данных. Эксплуатация уязвимости может позволить нарушителю получить полный доступ к программному обеспечению с правами группы confluence-users.

В случае невозможности установки обновления данного программного обеспечения необходимо удалить или отключить учетную запись disabledsystemuser.

23. Устранение уязвимости компонента Velocity Template Handler веб-сервера Atlassian Confluence Server и дата центра Confluence Data Center связана с ошибками при обработке входных данных (BDU:2022-04765, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанной с ошибками при генерации кода шаблона. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо приять следующие меры:

- использовать указанное программное обеспечение с минимально необходимым уровнем привилегий;

- ограничить использование библиотеки XStrem для работы с шаблонами с целью предотвращения внедрения в них вредоносного кода.

24. Устранение уязвимости пользовательского интерфейса платформы администрирования приложений VMware Workspace One Acces, консоли администрирования VMware Identity Manager (vIDM) и средства управления виртуальной инфраструктуры VMware vRealize Automation (BDU:2022-04799, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), связанная с возможностью обхода аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В случае необходимости установки обновления программного обеспечения необходимо приять следующие меры:

- сделать резервную копию базы данных Workspase ONE Access;

- выполнить приведенные ниже запросы к базе данных Workspase ONE Access;

- запустить View-Active-Admin-users.sql, чтобы получить перечень администраторов (включая администраторов только для чтения), и запустить View-Active-Local-users.sql, чтобы получить перечень локальных пользователей, которые будут отключены. Убедиться, что View-Active-Admin-users.sql показывает, как минимум 1 подготовленного (обычно из каталога) администратора;

- запустить Disable_All_Local_Users.sql, чтобы отключить всех локальных пользователей и администраторов;

- запустить View-Active-Admin-users.sql, чтобы узнать, какие администраторы сейчас остаются активными. Здесь долдоны отображаться только подготовленные (обычно пользователи каталога) администраторы userType;

- получить доступ к устройству Workspase ONE Access/VMware Identity Manager, используя sshclient в качестве пользователя root. Перезапустить службу с помощью команды service Horizon-Workspace Restart;

- повторить этот процесс для всех устройств среды;

- пока исправления не будут применены, рекомендуется не создавать, новых локальных пользователей.

25. Уязвимость средства организации удаленного доступа Kaspersky VPN Secure Connection (BDU:2022-04803, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – высокий), связанная с возможностью удаления произвольных файлов в системе. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии путем создания специально сформированной символической ссылки на критическую папку в системе и удаления ее с помощью функции «Удалить служебные данные и отчеты».

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление до версии Kaspersky VPN Secure Connection 21.6 и ограничить доступ пользователей к функциям «Удалить все служебные данные и отчеты» или «Сохранить отчет на вашем компьютере».

26. Устранение уязвимости системы управления базами данных PostgreSQL (BDU:2022-04971, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с ошибками при использовании расширениями команд OR. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии и заменить произвольные объекты в базе данных.

В целях предотвращения возможности эксплуатации данной уязвимости необходимо принять следующие меры:

- проверка расширений на возможность создания объектов в базе данных (убедитесь, что ни один из этих объектов не содержится в системе);

- отклонение неиспользуемых учетных записей, а также учетных записей недоверенных пользователей;

- использование входных данных только из доверенных источников.

27. Устранение уязвимости Java-библиотеки для преобразования объектов в XML или JSON формат XStream платформы виртуализации VMware Cloud Foundation (BDU:2022-06488, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с ошибками десериализации и возможностью внедрение кода. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с root-привилегиями.

В случае необходимости установки обновления программного обеспечения необходимо приять следующие меры:

-для Java библиотеки XStream использовать «белый» список объектов для десериализуемых данных из недоверенных источников и ограничить перечень обрабатываемых типов минимальной необходимости;

-для платформы виртуализации VMware Cloud Foundation использовать средства межсетевого экранирования для ограничения возможности загрузки недоверенных данных.

28. Уязвимость компонента Crash Report функции sigsevgHandler файла debug.c системы управления базами данных Redis (BDU:2022-06489, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с

некорректной зачисткой или освобождением ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

В случае невозможности установки обновления данного программного обеспечения необходимо:

-использовать средства антивирусной защиты;

-использовать средства межсетевого экранирования с целью ограничения возможности получения доступа к базе данных.

29. Уязвимость функции unwrap_des() и unwrap_des3 () библиотеки GSSAPI из пакета Heimdal программы сетевого взаимодействия Samba (BDU:2022-06493, уровень опасности по CVSS 2.0 –средний, по CVSS 3.0 – средний), связанная с переполнением буфера в стеке. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

В случае невозможности установки обновления данного программного обеспечения необходимо:

-компилировать Samba с параметром – with-system mitkrb5;

-использовать антивирусные средства защиты;

-использовать средства межсетевого экранирования.

30. Уязвимость пакета программ сетевого взаимодействия Samba (BDU:2022-06494, уровень опасности по CVSS 2.0 –средний, по CVSS 3.0 – средний), связанная с ошибками при обработке символических ссылок. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к файловой системе сервера.

В случае невозможности установки обновления данного программного обеспечения необходимо:

-отключить SMB1 для ограничения возможности создания символических ссылок;

-если для обратной совместимости необходимо включить SMB1, то необходимо добавить параметр *unix extensions = no* в раздел [global] вашего smb.conf и перезапустить smbd;

-рекомендуется экспортировать области файловой системы только по SMB2 или NFS, но не по обоим протоколам.

31. Уязвимость API-библиотеки системы управления базами данных SQLite (BDU:2022-06495, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), связанная с непроверенным индексированием массива. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В случае невозможности установки обновления данного программного обеспечения необходимо:

-использовать средства межсетевого экранирования уровня веб-приложений;

-ограничить возможность загрузки входных данных размером более 1 ГБ.

32. Уязвимость службы Active Directory Domain Service (BDU:2022-06580, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В случае невозможности установки обновления данного программного обеспечения необходимо:

-ограничить доступ из внешних сетей (Интернет);

-использовать средства межсетевого экранирования.