Рекомендации по недопущению взлома сайтов и веб-приложений органов государственной власти Республики Дагестан

1. Для сайтов:

Уязвимости, приводящие к инцидентам информационной безопасности в информационной сфере, классифицируются на 2 вида:

1.1. уязвимости, связанные с устаревшими версиями модулей и плагинов, содержащих ошибки безопасности в коде, скриптах, используемых на сайте;

1.2. утечка информации о реквизитах доступа к административной панели, вследствие наличия вредоносного программного обеспечения на локальном компьютере и использования протоколов передачи данных без шифрования.

Необходимые меры защиты:

1.1.1. использовать на хостинге сертифицированных средств межсетевого экранирования и антивирусной защиты.

1.1.2. обновить системы управления CMS и ее плагинов до актуальных версий.

1.1.3. изменить пароли доступа к панели управления, FTP, административной части сайтов и баз данных. Рекомендации к парольной защите: длина пароля – не менее 8 символов, включающих не менее одного символа прописной буквы английского алфавита (от A до Z), не менее одного символа строчной буквы английского алфавита (от a до z), не менее одного символа десятичной цифры (от 0 до 10) и не менее одного неалфавитного символа (@, #, $, &, *, % и т.п.). Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd и т.п.).

1.1.4. использовать безопасные протоколы передачи данных с шифрованием (SSH, SFTP, HTTPS).

1.1.5. настроить регулярное выполнение резервного копирования для оперативного восстановления сайта в случае взлома.

1.1.6. отключить на сайтах сервисы иностранных разработчиков, в том числе сервисы детальной статистики.

1.1.7. настроить правила доступа для всех категорий пользователей веб-серверов к файлам и каталогам веб-сервера в соответствии с установленными правилами разграничения доступа (например, для пользователей, от имени которых запускается веб-сервер, для пользователей ftp-серверов и пользователей других служб).

1.1.8. установить минимально необходимые для работы правила доступа к файлам и директориям веб-серверов пользователям и администраторам.

1.1.9. ограничить доступ к каталогам систем контроля версий и их содержимому (таким как .git, .svn и другим каталогам), которые осуществляют сканирование.

1.1.10. настроить запрет выдачи листинга каталогов при отсутствии в них индексируемых файлов (если иное не предусмотрено функциональными возможностями веб-сервера).

1.1.11. настроить с использованием файла с именем robots.txt разрешенные и запрещенные для индексации каталоги, и файлы.

1.1.12. ограничить хранение в директориях веб-сервера резервных копий и прочих файлов, наличие которых не требуется для функционирования веб-приложения.

1.1.13. ограничить использование на веб-страницах серверов информационных ресурсов (видеофайлов, электронных документов, изображений и других файлов), размещенных на сторонних серверах.

2. Для веб-приложений:

2.1. Использовать защищенные протоколы TLS v1.2 (и выше) при прохождении процедуры аутентификации пользователей в веб-приложении.

2.2. Запретить предоставлять в выводе сообщений об ошибках следующую информацию:

- данные о структуре файловой системы (информация о версии операционной системы, директориях с системными файлами и системным программным обеспечением, включая пути к директориям и файлам);

- фрагменты программного или конфигурационного кода;

- сообщения об ошибках при передаче запросов в СУБД;

- SQL-выражения, используемые при доступе к базе данных.

2.3. Выдавать пользователю страницу-заглушку с кодом HTTP-ответа веб-сервера «200» при обработке ошибок веб-сервером.

2.4. По возможности ограничить использование при обработке веб-сервером данных в формате XML внешних сущностей (External Entity), внешних параметров сущностей (External Parameter Entity) и внешних описаний типа документа (External Doctype), а также JSON.

2.5. Запретить кеширование веб-форм ввода конфиденциальной информации. Выставить атрибут HTTPOnly у параметров cookie, значения которых не должны быть доступны сценариям, выполняемым браузером. У параметров cookie, содержащих чувствительную информацию, необходимо выставить атрибут secure.

2.6. Проводить проверку корректности вводимых пользователем данных как на стороне клиента (с использованием сценариев, исполняемых браузером), так и на стороне сервера.

2.7. Использовать директивы в заголовках сообщений HTTP, определяющие применяемую кодировку. Исключить использование разных кодировок для разных источников входных данных.

2.8. Использование параметризованные запросы (например, хранимые процедуры) для построения SQL-запросов. В случае отсутствия такой возможности, организовать процедуру предварительной обработки получаемых от пользователей данных (путем удаления «` – / *», а также следующих SQL-операторов: SELECT, UNION, ALTER, UPDATE, EXEC, DROP, DELETE и INSERT).

2.9. Осуществлять преобразование HTML-кода входного потока данных следующим образом:

- заменить < > на &lt и >

- заменить ( ) на &#40 и)

- заменить # на #

- заменить & на &#38.

2.10. Осуществлять фильтрацию входного потока данных (например, с использованием методов Server.HTMLEncode и HttpServerUtility.HTMLEncode в ASP и ASP.NET).

2.11. Запретить пользователю ввод данных, в которых допустимы HTML-теги <IMG> или <TABLE>.

2.12. Для подсистем разграничения сессиями пользователей:

- организовать авторизованному пользователю веб-приложения возможность самостоятельного завершения сеанса работы в веб-приложении;

- обеспечить гарантированное удаление идентификатора соответствующей сессии по завершении сеанса работы клиента веб-приложения;

- ограничить время жизни активной сессии пользователя.

2.13. Для подсистем разграничения доступа:

- организовать доступ к защищенным ресурсам веб-приложения только после прохождения процедуры аутентификации;

- обеспечить хранение аутентификационных данных пользователей веб-приложения только в криптографически защищенном виде;

- исключить хранение аутентификационных данных (от веб-приложений, СУБД, ТКО, FTP и т.п.) в файлах конфигурации, доступных путем обращения к ним по URL;

- исключить хранение в HTML-страницах аутентификационных данных, а также информации, позволяющей сделать вывод о структуре каталогов веб-приложения на веб-сервере;

- в случае, если в веб-приложении предусматривается возможность внесения изменений пользователем в принадлежащий ему профиль, внесенные изменения необходимо подтверждать дополнительной процедурой аутентификации;

- запретить использование заголовка REFERER в качестве основного механизма авторизации.

2.14. Отказаться от использования на веб-ресурсах (в том числе веб-сайтах) компонентов и контента, подгружаемых с внешних, не контролируемых организацией, ресурсов.

2.15. В случае невозможности отказа от использования указанных компонентов и контента, осуществлять их проверку на предмет вредоносного воздействия на отображаемую в браузерах пользователя информацию и возможность кражи аутентификационных данных и файлов-cookie пользователей. Далее осуществлять периодическую проверку их хэш-сумм.

В случае изменения хэш-сумм - блокировать использование указанных компонентов и контента на веб-ресурсе и осуществлять их повторную проверку функциональности. В случае отсутствия потенциально вредоносного функционала-поводить дальнейшее сравнение по новой хэш-сумме.

3. Для программной платформы:

3.1. Уязвимость параметра conf_id программного обеспечения TrueConf Server, связанная с возможностью обхода пути в сценарии /client/upsld/v1 (BDU:2022-03309, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический). Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код путем записи специально сформированного php-файла в папку доступную через веб-интерфейс.

3.2. Уязвимость программного обеспечения TrueConf Server, связанная с

возможностью обхода пути в сценарии /handlers/get-img-file.php (BDU:2022-03308, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий). Эксплуатация уязвимости может позволить нарушителю получить доступ к произвольным файлам.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо обновить программное обеспечение до актуальной версии (4.7.3 или 5.0.2).

3.3. Уязвимость компонента Velocity Template Handler веб-сервера Atlassian Confluence Server и дата центра Confluence Data Center (BDU:2022-04765, уровень опасности по CVSS 2.0 – высокий уровень опасности, по CVSS 3.0 – высокий уровень опасности), 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 принять меры:

-использовать указанное ПО с минимально необходимым уровнем привилегий;

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

3.4. Устранения уязвимости приложения Questions for Confluence веб-сервера Atlassian Confluence Server и дата центра Confluence Data Center (BDU:2022-04612, уровень опасности по CVSS 2.0 – высокий уровень опасности, по CVSS 3.0 – высокий уровень опасности), 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 ПО необходимо удалить или отключить учетную запись disabledsystemuser.

3.5. Уязвимость веб-интерфейса платформы управления политиками соединений Cisco Identity Engine (BDU:2022-06490, уровень опасности по CVSS 2.0

– высокий уровень опасности, по CVSS 3.0 – высокий уровень опасности), связанная с недостаточной проверкой входных данных. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, читать и изменять файлы на уязвимом устройстве путем отправки специального сформированного HTTP-запроса.

В случае невозможности установки обновления ПО необходимо принять следующие меры:

-ограничить доступ из внешних сетей «Интернет»;

-использовать средства межсетевого экранирования уровня приложений.

3.6. Уязвимость веб-интерфейса платформы управления политиками соединений Cisco Small Business RV016, RV042, RV042G и RV082 (BDU:2023-00167, уровень опасности по CVSS 2.0 – критический уровень опасности, по CVSS 3.0 – критический уровень опасности), связанная ошибками при управлениях привилегиями. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, получить root-доступ к базовой операционной системе.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо принять меры:

-отключить удаленное управление:

1.войти в веб-интерфейс управления устройством;

2.выбрать «Брендмауэр» > «Основные»;

3.снять флажок «Удаленное управление»;

4.блокировать доступ к портам 443 и 60443»;

5.использовать средства межсетевого экранирования уровня веб-приложений.