АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ АЛЕКСАНДРОВСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН ВЛАДИМИРСКОЙ ОБЛАСТИ
ул. Красной молодежи, дом 7,
г. Александров, Владимирская обл., 601650
тел. 2-21-31, факс. 2-21-40,
e-mail: alexan@avo.ru
ОКПО 04023819, ОГРН 1033303207024, ИНН 3311004500

от 16.11.2023 №01-08-2142

на № ..... от .....

Главам администраций городских
и сельских поселений

Руководителям муниципальных учреждений

О мерах по повышению защищенности информационной инфраструктуры

В соответствии с письмом от 14.11.2023 № УЗГТИ-407-13-10 администрации Губернатора Владимирской области направляю информационное сообщение о мерах по повышению защищенности информационной инфраструктуры органов местного самоуправления.

Прошу направляемую информацию оперативно довести до сотрудников, отвечающих за обеспечение защиты информации.

Направляется в порядке информирования для принятия мер реагирования.

Приложение: Меры по повышению защищенности информационной инфраструктуры на 2 л. в 1 экз.

Заместитель главы администрации
по вопросам социальной политики, культуры и спорта И.К. Сергеева

Исаев Андрей Владимирович
(49244) 2-27-16

Приложение

Меры по повышению защищенности информационной инфраструктуры

1. Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками в адрес федеральных органов исполнительной власти и организаций Российской Федерации направляются фишинговые письма, содержащие вредоносные вложения в виде ссылок на вредоносные файлы с расширением .exe или .scr, которые маскируются под документы Microsoft Word (.doc, .docx) или PDF.

С целью обеспечения устойчивого функционирования автоматизированных рабочих мест, имеющих доступ в сеть «Интернет», и предотвращения реализации угроз безопасности информации, связанных с фишингом, необходимо проинформировать работников органа исполнительной власти (организации) о необходимости:

проверки адреса отправителя, даже в случае совпадения имени с уже известным контактом;

проверки писем, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

проверки ссылок, содержащихся в электронном письме, даже если письмо получено от другого пользователя информационной системы;

внимательного отношения к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками.

Создать отдельный электронный почтовый адрес, на который пользователи информационной системы будут присылать письма, которые могут содержать вредоносное содержание (ссылку или вложение).

Организовать отправку подозрительных писем, получаемых пользователями почтового сервиса, на единый (отдельный) электронный почтовый адрес для их проверки администратором безопасности. При возможности для этих целей использовать почтовую «песочницу».

Осуществлять проверку всех поступающих на почту вложений

с использованием средств антивирусной защиты, антиспама (при наличии). Обновить базы антивирусных средств защиты до актуальных версий.

Использовать для работы с электронной почтой учетные записи пользователей операционной системы с минимальными возможными привилегиями.

Активировать механизмы проверки электронной почты, проверки подлинности домена-отправителя (например, использовать технологии DKIM,

DMARC, SPF), а также настроить проверку входящих писем с использованием этих технологий (в соответствии с рекомендациями ФСТЭК России от 18 июля 2023 г. № 240/22/3456).

Заблокировать (при возможности) получение пользователями информационной системы в электронных письмах вложений с расширениями ADE, ADP, .APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH.

Организовать (при возможности) доставку писем от доменов-отправителей по «белым» или «черным» спискам.

В случае, если организация не взаимодействует с иностранными контрагентами, запретить коммуникации на сетевом уровне по протоколу SMTP с зарубежными IP-адресами.

Настроить функции уведомления пользователей в тексте сообщения при получении электронного письма от внешнего отправителя.

2. Уязвимость функции nvmet_tcp_free_crypto файла drivers/nvme/target/tcp.c подсистемы NVMe-oF/TCP ядра операционных систем Linux (BDU:2023-06750, уровень опасности по CVSS 3.0 — высокий), связанная с возможностью использования памяти после освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии или выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi).

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

произвести минимизацию пользовательских привилегий;

отключить (удалить) неиспользуемые учётные записи пользователей;

использовать средства межсетевого экранирования для ограничения возможности удалённого доступа.