МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЧЕЧЕНСКОЙ РЕСПУБЛИКИ
(Минобрнауки ЧР)

ул. им. академика М.Д. Миллионщикова, 67 «а»,
г. Грозный, Чеченская Республика, 364021,
тел.: 8 (8712) 22-27-42, факс: 22-51-88
E-mail: mail@mon95.ru
http://www.mon 95.ru
ОКПО 45266617, ОГРН 1022002542737
ИНН/КПП 2020001415/201401001

НОХЧИЙН РЕСПУБЛИКИН ДЕШАРАН А, ЙИЛМАНАН А МИНИСТЕРСТВО

академикан М.Д. Миллионщиковн ц1арах урам, 67«а»
Соьлжа-Г1ала, Нохчийн Республика, 364021,
тел.: 8 (8712) 22-27-42, факс: 22-51-88
E-mail: mail@mon95.ru
http://www.mon 95.ru
ОКПО 45266617, ОГРН 1022002542737
ИНН/КПП 2020001415/201401001

19.01.2023 № 40/07-43
На № _____ от _____

Руководителям органов управления образованием муниципальных районов и городских округов Чеченской Республики

Руководителям образовательных организаций и государственных учреждений, подведомственных Министерству образования и науки Чеченской Республики

Министерство образования и науки Чеченской Республики сообщает о том, что анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает активизацию зарубежных хакерских группировок по реализации компьютерных атак на информационную инфраструктуру Российской Федерации. При этом активно эксплуатируются уязвимости программного обеспечения.

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, просим обратить внимание на необходимость устранения следующих уязвимостей:

1. Уязвимость SSL-VPN-портала операционной системы ForliOS (BDU.2022- 07226, уровень опасности по CVSS 2.0 - критический уровень опасности, по CVSS 3.0 - критический уровень опасности), связанная с переполнением буфера на основе кучи. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 г. (fstec.ni/tekhnicheskaya-zashchita-mfomiatsii/dokumenty/l 14-spetsialnye-nonnativnye- dokumenty).

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

отключить SSL-VPN;

использовать средства межсетевого экранирования для формирования «белого» списка адресов, которым разрешен удаленный доступ;

использовать системы обнаружения вторжений для отслеживания известных индикаторов компрометации:

1.1 Записей в журналах дотирований:

Logdesc= "Application crashed" and msg= "[...] application:sslvpnd,[...], Signal I I received,Backtrace: [...].

1.2 Артефактов в файловой системе:

/data/lib/libips.bak
/data/lib/libgif.so
/data/lib/libiptcp.so
/data/lib/Iibipudp.so
/data/lib/libjepg.so
/var/ sslvpnconftgbk
/data/etc/wxd.conf.
/flash

1.3 Подключений к скомпромеитированным IP-адресам:
188.34.130.40:444;
103.131.189.143:30080,3 0081,3 0443,20443;
192.36.119.61:8443,444;
172.247.168.153:8033.

2. Уязвимость в функции audin_send_open сервера xrdp семейства операционных систем Linux (BDU:2022-07224, уровень опасности по CVSS 2.0 - критический уровень опасности, по CVSS 3.0 — критический уровень опасности), связанная с возможностью переполнения буфера в стеке.

Уязвимость в функции xrdp_mmJrans_process_drdynvc_channel_opcn (BDU:2022-07224, уровень опасности по CVSS 2.0 - критический уровень опасности, по CVSS 3.0 - критический уровень опасности), связанная с возможностью записи за пределами буфера в памяти.

Эксплуатация указанных уязвимостей может позволить нарушителю, действующему удаленно, получить доступ к удаленной машине.

В целях предотвращения возможности эксплуатации указанных уязвимостей рекомендуется установить обновление профаммного обеспечения в соответствии с Методикой оценки уровня критичности

программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 г. (fstec.ru/tekhnicheskaya-zashchita-infomiatsii/dokunienty/114-spetsialnye-normativnye- dokumenty).

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

отключить сервер xrdp;

ограничить возможность доступа к портам, используемым для организации удаленного доступа (порт: 3389);

использовать средства межсетевого экранирования для формирования «белого» списка адресов, которым разрешен удаленный доступ.

Рекомендуем принять необходимые меры по устранению вышеперечисленных уязвимостей. Также просим довести данную информацию до всех подведомственных организаций.

Начальник информационного отдела - Пресс-секретарь Х.А. Маликов

Зубайраева Медина Идрисовна, информационный отдел, главный специалист-эксперт
8 (8712)22-61-18, mon-info@mail.ru