МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ

Рашпилевская ул., д. 23, г. Краснодар, 350063
Тел. (861) 298-25-73, (861)298-26-00
E-mail: minobrkuban@krasnodar.ru

05.04.2022 № 47-01-13-5790/22

На № _____ от _____

Руководителям муниципальных органов управления образованием Краснодарского края

Руководителям государственных (муниципальных) образовательных организаций Краснодарского края

О повышении уровня защищенности

На основании информации, полученной от Управления ФСТЭК России по Южному и Северо-Кавказскому округу, министерство образования, науки и молодежной политики Краснодарского края (далее - министерство) сообщает, что зарубежными хакерскими группировками при реализации компьютерных атак на информационную инфраструктуру Российской Федерации активно эксплуатируются уязвимости иностранного программного обеспечения.

С целью повышения уровня защищенности информационной инфраструктуры региональной мультисервисной сети исполнительных органов государственной власти Краснодарского края (далее – РМС ОГВ), а также информационной инфраструктуры исполнительных органов государственной власти Краснодарского края и органов местного самоуправления Краснодарского края, не входящей в централизованную структуру РМС ОГВ в части предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, министерство просит обратить внимание на необходимость устранения следующих уязвимостей:

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-OS (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:202200972, 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 (BDU2022-00995, 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.

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.

Первый заместитель министра

Подлинник электронного документа, подписанного электронной подписью, хранится в системе электронного документооборота администрации Краснодарского края
Сертификат 5CED30EB12110DC45C30A0365B084B17F999543E
Владелец **Пронько Сергей Валентинович**
Действителен с 26.01.2021 по 26.04.2022

С.В. Пронько

Платонова Алла Владимировна
+7(861)298-25-89