НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210118.1 | 18 января 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Mk-Auth

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Mk-Auth: 19.01
Дата выявления	29 июня 2020 г.
Дата обновления	4 января 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-14068	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в central/executar_login.php. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода) Рекомендации по устранению: обновить программное обеспечение.	9.1

MITRE: CVE-2020-14070	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД с привилегиями администратора к целевой системе. Уязвимость обусловлена наличием предполагаемых учетных данных в admin/executar_login.php. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-255: Уязвимости, связанные с управлением учетными данными Рекомендации по устранению: обновить программное обеспечение.	9.1

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021010401 http://mk-auth.com.br/page/changelog-1 https://gist.github.com/merhawi023/a1155913df3cf0c17971b0fb7dcd8f20