НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200428.4 | 28 апреля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Kiali

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Kiali до v1.15.0
Дата выявления	25 марта 2020 г.
Дата обновления	28 апреля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-1762	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к данным посредством использования скомпрометированного токена доступа (JWT cookie). Уязвимость обусловлена недостаточной проверкой предоставленных пользователем файлов JWT cookie. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:U/RL:O/RC:C CWE-613: Некорректно настроенный срок действия сессий Рекомендации по устранению: обновить программное обеспечение.	9.4

MITRE: CVE-2020-1764	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить несанкционированный доступ к данным посредством создания самоподписанных токенов доступа (JWT cookie). Уязвимость обусловлена наличием неизменяемого криптографического ключа в конфигурационном файле. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:U/RL:O/RC:C CWE-321: Использование жестко закодированного ключа шифрования Рекомендации по устранению: обновить программное обеспечение.	9.4

Ссылки на источники	https://kiali.io/news/security-bulletins/kiali-security-001/ https://www.cybersecurity-help.cz/vdb/SB2020042807