НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210118.6 | 18 января 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Некорректная аутентификация в GitLab

Идентификатор уязвимости	MITRE: Не определен
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством использования API-токена доступа другого пользователя. Уязвимость обусловлена некорректной проверкой параметров аутентификации на странице GitLab.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Gitlab Community Edition до v13.7.2, 13.6.4 и 13.5.6 GitLab Enterprise Edition до v13.7.2, 13.6.4 и 13.5.6
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 января 2021 г.
Дата обновления	8 января 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкий (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021010811 https://about.gitlab.com/releases/2021/01/07/security-release-gitlab-13-7-2-released/