НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211130.10 | 30 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Сброс пользовательских паролей в Team Password Manager

Идентификатор уязвимости	MITRE: CVE-2021-44037
Идентификатор программной ошибки	CWE-640: Ненадежный механизм восстановления забытого пароля
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику сбросить пароль пользователя. Уязвимость обусловлена некорректной работой механизма восстановления пароля.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Team Password Manager: до 10.135.236
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	26 ноября 2021 г.
Дата обновления	26 ноября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (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)	Отсутствует (N)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Отсутствует (N)

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/SB2021112612 http://teampasswordmanager.com/docs/changelog/#10.135.236 http://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-060.txt