НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20221021.15 | 21 октября 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Git

Идентификатор уязвимости	MITRE: CVE-2022-39260
Идентификатор программной ошибки	CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе посредством выполнения пользователем специально созданного вредоносного кода из репозитория. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Git: 2.38.0, 2.37.0 - 2.37.3, 2.36.0 - 2.36.2, 2.35.0 - 2.35.4, 2.34.0 - 2.34.4, 2.33.0 - 2.33.4, 2.32.0 - 2.32.3, 2.31.0 - 2.31.4, 2.30.0 - 2.30.5
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	19 октября 2022 г.
Дата обновления	19 октября 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.5 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Низкий (L)

Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	http://github.com/git/git/security/advisories/GHSA-rjr6-wcq6-83p6