НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220812.34 | 12 августа 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Выполнение произвольного кода в Zlib

Идентификатор уязвимости	MITRE: CVE-2022-37434
Идентификатор программной ошибки	CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Zlib: 0.8 - 1.2.12
Рекомендации по устранению	Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами
Дата выявления	7 августа 2022 г.
Дата обновления	7 августа 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
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	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	http://github.com/nodejs/node/blob/75b68c6e4db515f76df73af476eccf382bbcb00a/deps/zlib/inflate.c#L762-L764 http://github.com/ivd38/zlib_overflow http://github.com/madler/zlib/commit/eff308af425b67093bab25f80f1ae950166bece1 http://github.com/madler/zlib/blob/21767c654d31d2dccdde4330529775c6c5fd5389/zlib.h#L1062-L1063 http://www.openwall.com/lists/oss-security/2022/08/05/2