НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211229.6 | 29 декабря 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд оболочки в Gnome GEGL

Идентификатор уязвимости	MITRE: CVE-2021-45463
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	gegl: до 0.4.32
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	28 декабря 2021 г.
Дата обновления	28 декабря 2021 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	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021122817 http://gitlab.gnome.org/GNOME/gegl/-/commit/bfce470f0f2f37968862129d5038b35429f2909b http://gitlab.gnome.org/GNOME/gegl/-/blob/master/docs/NEWS.adoc http://gitlab.gnome.org/GNOME/gimp/-/commit/e8a31ba4f2ce7e6bc34882dc27c97fba993f5868 http://www.gimp.org/news/2021/12/21/gimp-2-10-30-released/