

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220812.6 | 12 августа 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в GNOME GDK-PixBuf

Идентификатор уязвимости	MITRE: CVE-2021-46829
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного GIF-изображения. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Gnome gdk-pixbuf: 2.0.0 - 2.90.3
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	8 августа 2022 г.
Дата обновления	8 августа 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/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)	Требуется (R)

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	http://gitlab.gnome.org/GNOME/gdk-pixbuf/-/commit/bca00032ad68d0b0aa2c1f7558db931e52bd9cd2 http://gitlab.gnome.org/GNOME/gdk-pixbuf/-/commit/5398f04d772f7f8baf5265715696ed88db0f0512 http://www.openwall.com/lists/oss-security/2022/07/23/1 http://gitlab.gnome.org/GNOME/gdk-pixbuf/-/issues/190 http://gitlab.gnome.org/GNOME/gdk-pixbuf/-/merge_requests/121 http://www.openwall.com/lists/oss-security/2022/07/25/1 http://github.com/pedrib/PoC/blob/master/fuzzing/CVE-2021-46829/CVE-2021-46829.md
---------------------	---