НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221101.7 | 1 ноября 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Libxml2

Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Libxml2: 2.0.0 - 2.10.2
Дата выявления	30 октября 2022 г.
Дата обновления	30 октября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-40304	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена возможностью обработки ссылочных циклов. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-399: Уязвимости, связанные с управлением ресурсами 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.	8.1

MITRE: CVE-2022-40303	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-190: Целочисленное переполнение или циклический возврат 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.	7.5

Ссылки на источники	http://gitlab.gnome.org/GNOME/libxml2/-/commit/ffaec75809a315457891a0e54f8828bc6e056067 http://gitlab.gnome.org/GNOME/libxml2/-/commit/644a89e080bced793295f61f18aac8cfad6bece2