# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210317.1 | 17 марта 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Выполнение произвольного кода в OpenJ9

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2020-27221 |
| Идентификатор программной ошибки | CWE-121: Переполнение буфера в стеке |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректным определением границ памяти при конвертации символов из кодировки UTF-8 в кодировку платформы. |
| Категория уязвимого продукта | Серверное программное обеспечение и его компоненты |
| Уязвимый продукт | IBM VIOS: 3.1.0, 3.1.1, 3.1.2<br>IBM AIX: 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.2.0, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 21 января 2021 г. |
| Дата обновления | 21 января 2021 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 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 | https://www.cybersecurity-help.cz/vdb/SB2021031602<br>https://bugs.eclipse.org/bugs/show_bug.cgi?id=569763 |