

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210708.1 | 8 июля 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в PHP

| | |
|--|--|
| Идентификатор уязвимости | MITRE: CVE-2021-21704 |
| Идентификатор программной ошибки | CWE-121: Переполнение буфера в стеке |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена переполнением буфера в функциях <code>firebird_info_cb()</code> , <code>firebird_handle_doer()</code> , <code>firebird_stmt_execute()</code> и <code>firebird_fetch_blob()</code> . |
| Категория уязвимого продукта | Универсальные библиотеки и компоненты |
| Уязвимый продукт | PHP: 7.3, 7.3.0, 7.3.0alpha1, 7.3.0alpha4, 7.3.0beta1, 7.3.0beta3, 7.3.1, 7.3.2, 7.3.3, 7.3.4, 7.3.5, 7.3.6, 7.3.7, 7.3.8, 7.3.9, 7.3.10, 7.3.11, 7.3.12, 7.3.13, 7.3.14, 7.3.15, 7.3.16, 7.3.17, 7.3.18, 7.3.19, 7.3.20, 7.3.21, 7.3.22, 7.3.23, 7.3.24, 7.3.25, 7.3.26, 7.3.27, 7.3.28, 7.4, 7.4.0, 7.4.1, 7.4.2, 7.4.3, 7.4.4, 7.4.5, 7.4.6, 7.4.7, 7.4.8, 7.4.9, 7.4.10, 7.4.11, 7.4.12, 7.4.13, 7.4.14, 7.4.15, 7.4.16, 7.4.18, 7.4.19, 7.4.20, 8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.5, 8.0.6, 8.0.7 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 6 июля 2021 г. |
| Дата обновления | 6 июля 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/SB2021070611 https://www.php.net/ChangeLog-8.php#8.0.8 https://www.php.net/ChangeLog-7.php#7.4.21 https://www.php.net/ChangeLog-7.php#7.3.29 http://bugs.php.net/76448 http://bugs.php.net/76449 http://bugs.php.net/76450 http://bugs.php.net/76452 |