# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210219.5 | 19 февраля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Удаленное выполнение кода в ISC BIND

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2020-8625 |
| Идентификатор программной ошибки | CWE-119: Выполнение операций за пределами буфера памяти |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного DNS-запроса. Уязвимость обусловлена некорректной реализацией механизма SPNEGO в расширении GSS-TSIG. |
| Категория уязвимого продукта | Серверное программное обеспечение и его компоненты |
| Уязвимый продукт | ISC BIND v9.5.0 - 9.11.27, 9.12.0 - 9.16.11, 9.11.3-S1 - 9.11.27-S1, 9.16.8-S1 - 9.16.11-S, 9.17.0 - 9.17.1 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 17 февраля 2021 г. |
| Дата обновления | 17 февраля 2021 г. |
| Оценка критичности уязвимости (CVSSv3.0) | 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://kb.isc.org/docs/cve-2020-8625<br>https://www.cybersecurity-help.cz/vdb/SB2021021718 |