НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230201.1 | 1 февраля 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ISC BIND

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	ISC BIND: 9.16.12 - 9.19.8
Дата выявления	25 января 2023 г.
Дата обновления	25 января 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-3924	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных в сервисе named. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-617: Несанкционированный вызов утверждения 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

MITRE: CVE-2022-3736	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных в сервисе named. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-20: Некорректная проверка входных данных 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
MITRE: CVE-2022-3094	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных в сервисе named. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) 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://kb.isc.org/docs/cve-2022-3924 http://kb.isc.org/docs/cve-2022-3094 http://kb.isc.org/docs/cve-2022-3736