

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

VULN-20200428.2 | 28 апреля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Удаленное выполнение кода в Apache IoTDB

Описание уязвимости Обусловлена отсутствием авторизации для порта ЈМХ 31999.  Категория уязвимого продукта Серверное программное обеспечение и его компоненты Обновить программное обеспечение Дата выявления Дата обновления Обновить программное обеспечение Дата обновления Оторта ЈМХ 31999. Оценка критичности уязвимости (CVSSv3.1) Оценка критичности уязвимости (CVSSv3.1) Оценка критичности уязвимости (CVSSv3.1) Оторта дого г. Оценка критичности уязвимости (СVSSv3.1) Оторта дого г. Оценка критичности уязвимости (О) Отортствует (N) Отортствует (N) Необходимость взаимодействия с оторта дого г. Отортствует (N) Необходимость взаимодействия с оторта дого г. Отортствует (N) Высокое (Н)	Идентификатор уязвимости	MITRE: CVE-2020-1952
Описание уязвимости  Категория уязвимого продукта  Серверное программное обеспечение и его компоненты  Уязвимое ПО  Арасће ІоТDBI до v0.9.2  Рекомендации по устранению  Обновить программное обеспечение  Дата выявления  27 апреля 2020 г.  Дата обновления  Оценка критичности уязвимости (CVSSv3.1)  Вектор атаки (AV)  Сетевой (N)  Сложность эксплуатации уязвимости (AC)  Необходимый уровень привилегий (PR)  Отсутствует (N)  Необходимость взаимодействия с пользователем (UI)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Идентификатор программной ошибки	CWE-285: Некорректная авторизация
Уязвимое ПО Арасhе IоTDBI до v0.9.2  Рекомендации по устранению Обновить программное обеспечение Дата выявления 27 апреля 2020 г.  Дата обновления 27 апреля 2020 г.  Оценка критичности уязвимости (CVSSv3.1) 9.8 AV:N/AC:L/PR:N/UI:N/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)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Описание уязвимости	злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена отсутствием авторизации для
Рекомендации по устранению  Дата выявления  27 апреля 2020 г.  Дата обновления  27 апреля 2020 г.  Оценка критичности уязвимости (CVSSv3.1)  Вектор атаки (AV)  Сетевой (N)  Сложность эксплуатации уязвимости (AC)  Необходимый уровень привилегий (PR)  Необходимость взаимодействия с пользователем (UI)  Масштаб последствий эксплуатации уязвимости (S)  Обновить программное обеспечение  27 апреля 2020 г.  27 апреля 2020 г.  Отенька критичности уязвимости (CVSSv3.1)  9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H  Сетевой (N)  Стетевой (N)  Отсутствует (N)  Необходимость взаимодействия с Отсутствует (N)  Не изменяется (U)	Категория уязвимого продукта	
Дата выявления27 апреля 2020 г.Дата обновления27 апреля 2020 г.Оценка критичности уязвимости (CVSSv3.1)9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:HВектор атаки (AV)Сетевой (N)Сложность эксплуатации уязвимости (AC)Низкая (L)Необходимый уровень привилегий (PR)Отсутствует (N)Необходимость взаимодействия с пользователем (UI)Отсутствует (N)Масштаб последствий эксплуатации уязвимости (S)Не изменяется (U)	Уязвимое ПО	Apache IoTDBI до v0.9.2
Дата обновления 27 апреля 2020 г.  Оценка критичности уязвимости (CVSSv3.1) 9.8 AV:N/AC:L/PR:N/UI:N/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)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Рекомендации по устранению	Обновить программное обеспечение
Оценка критичности уязвимости (CVSSv3.1) 9.8 AV:N/AC:L/PR:N/UI:N/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)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Дата выявления	27 апреля 2020 г.
Вектор атаки (AV)  Сложность эксплуатации уязвимости (AC)  Низкая (L)  Необходимый уровень привилегий (PR)  Отсутствует (N)  Необходимость взаимодействия с пользователем (UI)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Дата обновления	27 апреля 2020 г.
Сложность эксплуатации уязвимости (АС) Низкая (L)  Необходимый уровень привилегий (РR) Отсутствует (N)  Необходимость взаимодействия с пользователем (UI)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Необходимый уровень привилегий (PR)  Необходимость взаимодействия с Отсутствует (N)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Вектор атаки (AV)	Сетевой (N)
Необходимость взаимодействия с пользователем (UI)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Сложность эксплуатации уязвимости (АС)	Низкая (L)
пользователем (UI)  Масштаб последствий эксплуатации уязвимости (S)  Не изменяется (U)	Необходимый уровень привилегий (PR)	Отсутствует (N)
уязвимости (S) Не изменяется (U)	• • • • • • • • • • • • • • • • • • • •	Отсутствует (N)
Влияние на конфиденциальность (С) Высокое (Н)		Не изменяется (U)
	Влияние на конфиденциальность (С)	Высокое (Н)

Влияние на целостность (I)	Высокое (Н)
Влияние на доступность (А)	Высокое (Н)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-1952 https://www.cybersecurity-help.cz/vdb/SB2020042720 https://seclists.org/oss-sec/2020/q2/73