

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200518.4 | 18 мая 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Уязвимость отказа в обслуживании в обработчике Bitdefender

Идентификатор уязвимости	MITRE: CVE-2020-8100
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством сканирования ABC специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных в модуле sevakrnl.rv0.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Bitdefender Engines до v7.84063
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 мая 2020 г.
Дата обновления	15 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокий (H)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
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.bitdefender.com/support/security-advisories/incomplete-validation-detection-code-bitdefender-engines-va-8589/>

<https://nvd.nist.gov/vuln/detail/CVE-2020-8100>