

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200602.5 | 2 июня 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **НЕТ**

Инъекция SQL-команд в Online-Exam-System

Идентификатор уязвимости	Не определен
Идентификатор программной ошибки	CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (Внедрение SQL-кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольные SQL-запросы к базе данных уязвимого приложения. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных в параметре «fid» в файле «dash.php»
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Online-Exam-System 2015
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	1 июня 2020 г.
Дата обновления	1 июня 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)	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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Отсутствует
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020060109