НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200603.2| 3 июня 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных кода в Inductive Automation Ignition

Идентификатор уязвимости	MITRE: CVE-2020-10644 CVE-2020-12000
Идентификатор программной ошибки	CWE-502: Десериализация недоверенных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством передачи специально сформированных вредоносных данных. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Ignition до v8.0.10
Рекомендации по устранению	Обновить программное обеспечение
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)	Низкий (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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.zerodayinitiative.com/advisories/ZDI-20-686/ https://www.zerodayinitiative.com/advisories/ZDI-20-687/ https://www.us-cert.gov/ics/advisories/icsa-20-147-01