

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200623.1 | 23 июня 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Множественные уязвимости в ПО ICONICS BizViz

Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимое ПО	BizViz до v9.5
Дата выявления	19 июня 2020 г.
Дата обновления	19 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-12007	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного сетевого пакета на сервер FrameWorX. Уязвимость обусловлена некорректной проверкой при обработке сериализованных данных в компоненте GenBroker64 / GenBroker32.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-502: Десериализация недоверенных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	9.8

<p>MITRE: CVE-2020-12013</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных в целевой системе посредством использования специально созданного вредоносного клиента WCF, взаимодействующего с сервером FrameWorX и выполняющего произвольные SQL-команды в базе данных уязвимого приложения. Уязвимость обусловлена некорректной работой с пользовательскими данными компонента GenBroker64 / GenBroker32.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	<p>9.8</p>
<p>MITRE: CVE-2020-12009 CVE-2020-12015</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально созданного вредоносного сетевого пакета. Уязвимость обусловлена некорректной проверкой при обработке сериализованных данных в компоненте GenBroker64 / GenBroker32.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:U/RC:C CWE-502: Десериализация недоверенных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	<p>7.5</p>
<p>MITRE: CVE-2020-12011</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного сетевого пакета. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных в компоненте GenBroker64 / GenBroker32.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-787: Запись за границами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	<p>8.1</p>

Ссылки на источники <https://www.us-cert.gov/ics/advisories/icsma-20-170-01>  
<https://www.cybersecurity-help.cz/vdb/SB2020061921>