НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200623.10 | 23 июня 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в ПО ICONICS

Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимое ПО	Hyper Historian до v10.96
Дата выявления	19 июня 2020 г.
Дата обновления	19 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-12013	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных 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. 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) Рекомендации по устранению: на данный момент отсутствуют.	9.8

MITRE: CVE-2020-12007	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. 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 Рекомендации по устранению: на данный момент отсутствуют.	9.8
MITRE: CVE-2020-12011	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного сетевого пакета на сервер FrameWorX. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных в компоненте GenBroker64 / GenBroker32. 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 Рекомендации по устранению: на данный момент отсутствуют.	8.1
MITRE: CVE-2020-12015 CVE-2020-12009	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать состояния отказа в обслуживании в целевой системе посредством отправки специально созданного вредоносного сетевого пакета. Уязвимость обусловлена некорректной проверкой при обработке сериализованных данных в компоненте GenBroker64 / GenBroker32. 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 Рекомендации по устранению: на данный момент отсутствуют.	7.5

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020061915 https://www.us-cert.gov/ics/advisories/icsa-20-170-03