НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220214.15 | 14 февраля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Schneider Electric IGSS Data Server

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	IGSS Data Server: 15.0.0.22020
Дата выявления	14 февраля 2022 г.
Дата обновления	14 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-24313	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе.Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2022-24314 CVE-2022-24315	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена граничным условием в процессе IGSSdataServer. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2022-24310	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-190: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение	9.8
MITRE: CVE-2022-24311 CVE-2022-24312	Эксплуатация уязвимости позволяет удаленному злоумышленнику заменять файлы в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение	7.5

Ссылки на источники	http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-039-01 https://www.cybersecurity-help.cz/vdb/SB2022021405 http://www.zerodayinitiative.com/advisories/ZDI-22-321/ http://www.zerodayinitiative.com/advisories/ZDI-22-322/ http://www.tenable.com/security/research/tra-2022-02 http://www.zerodayinitiative.com/advisories/ZDI-22-320/ http://www.zerodayinitiative.com/advisories/ZDI-22-325/