НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220610.4 | 10 июня 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Fortinet FortiAnalyzer

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	FortiAnalyzer: 6.4.0 - 6.4.7, 7.0.0 - 7.0.2
Дата выявления	07 июня 2022 г.
Дата обновления	07 июня 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-13927	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные API запросы в уязвимом приложении. Уязвимость обусловлена настройкой по умолчанию экспериментального API Airflow, позволяющей выполнять все запросы API без аутентификации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-287: Некорректная аутентификация Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.8

MITRE: CVE-2020-11982	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных в уязвимое приложение. Уязвимость обусловлена некорректной инициализацией внутренней переменной. CVSSv3.0: AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-453: Небезопасная инициализация переменной по умолчанию Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	8.5
MITRE: CVE-2020-11981	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных в уязвимое приложение. Уязвимость обусловлена некорректной проверкой входных данных в исполнителе "celery". CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	8.8

MITRE: CVE-2020-17526	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных в уязвимое приложение. Уязвимость обусловлена некорректным управлением сеансом в Apache Airflow на основе значения по умолчанию. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-798: Использование жестко закодированных учетных данных Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.1

Ссылки на источники	http://fortiguard.fortinet.com/psirt/FG-IR-22-008 https://nvd.nist.gov/vuln/detail/CVE-2020-13927