НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230306.1 | 6 марта 2023 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в FortiNAC

Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	FortiNAC: 8.3.7 - 9.4.0
Дата выявления	19 февраля 2023 г.
Дата обновления	22 февраля 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-39952	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить произвольные файлы в целевую систему посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена возможностью изменения имени или пути к файлу. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-73: Внешнее управление именем или путем файла 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-2022-40677	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H 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.	7.2
MITRE: CVE-2022-40678	Эксплуатация уязвимости позволяет локальному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированного запроса на восстановление пароля. Уязвимость обусловлена недостаточной защитой хранимых данных. CVSSv3.0: AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-522: Недостаточно надежная защита 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.	7.4

Ссылки на источники	http://fortiguard.com/psirt/FG-IR-22-300 http://fortiguard.com/psirt/FG-IR-22-265 http://fortiguard.com/psirt/FG-IR-22-280