НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210805.2 | 5 августа 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости Fortinet FortiPortal

Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	FortiPortal: 3.2.0, 3.2.1, 3.2.2, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.1.0, 4.1.1, 4.1.2, 4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.1.0, 5.1.1, 5.1.2, 5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 6.0.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4
Дата выявления	3 августа 2021 г.
Дата обновления	3 августа 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-32590	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных уязвимого приложения посредством отправки специально созданного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных. 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-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода) Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2021-32588	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды от имени пользователя root в целевой системе. Уязвимость обусловлена наличием жестко запрограммированного имени пользователя и пароля Tomcat Manager в коде приложения. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-798: Использование жестко закодированных учетных данных Рекомендации по устранению: обновить программное обеспечение	10.0
MITRE: CVE-2021-26104	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнять произвольные команды оболочки от имени пользователя root в целевой системе посредством использования специально созданных параметров команды CLI. Уязвимость обусловлена некорректной проверкой входных данных в интерфейсе командной строки. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/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: обновить программное обеспечение	8.8

Ссылки на источники	https://www.fortiguard.com/psirt/FG-IR-21-037 https://www.fortiguard.com/psirt/FG-IR-21-077 https://www.cybersecurity-help.cz/vdb/SB2021080312 https://www.fortiguard.com/psirt/FG-IR-21-084