

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220313.2 | 13 марта 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Zyxel Armor home routers

Идентификатор уязвимости	MITRE: CVE-2021-4029
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)
Описание уязвимости	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольные команды ОС в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	NBG6816 (Armor Z1): Все версии NBG6817 (Armor Z2): до 1.00(ABCS.11)C0
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.
Дата выявления	25 февраля 2022 г.
Дата обновления	февраля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)

Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены

Ссылки на источники

<https://www.cybersecurity-help.cz/vdb/SB2022022309>
<http://www.zyxel.com/support/forgery-vulnerabilities-of-select-Armor-home-routers.shtml>