

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210921.6 | 21 сентября 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **НЕТ**

Выполнение произвольных команд оболочки в Netgear R6020

Идентификатор уязвимости	MITRE: CVE-2021-41383
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных в скрипте setup.cgi в поле ntp_server.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	R6020: 1.0.0.48
Рекомендации по устранению	Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами
Дата выявления	21 сентября 2021 г.
Дата обновления	21 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
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	Наличие не подтверждено
Наличие средств устранения уязвимости	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены

Ссылки на источники

<https://www.cybersecurity-help.cz/vdb/SB2021092104>
<https://j-o-e-l-s.github.io/2021/09/15/Hacking-The-Netgear-R6020.html>