

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220914.31 | 14 сентября 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Zyxel NAS

Идентификатор уязвимости	MITRE: CVE-2022-34747
Идентификатор программной ошибки	CWE-134: Использование форматной строки, контролируемой извне
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного UPD-пакета. Уязвимость обусловлена ошибкой строки форматирования.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	NAS326: до V5.21(AAZF.11)C0 NAS540: до V5.21(AATB.8)C0 NAS542: до V5.21(ABAG.8)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	6 сентября 2022 г.
Дата обновления	6 сентября 2022 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	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	<a href="https://www.zyxel.com/support/Zyxel-security-advisory-for-format-string-vulnerability-in-NAS.shtml">https://www.zyxel.com/support/Zyxel-security-advisory-for-format-string-vulnerability-in-NAS.shtml</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-34747">https://nvd.nist.gov/vuln/detail/CVE-2022-34747</a>