НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210118.2 | 18 января 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в ПО Zyxel

Идентификатор уязвимости	Не определен
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке HTTP-запросов на веб-сервере zhttpd.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	EMG3525-T50B: до V5.50 (ABPM.4) C0, V5.50 (ABSL.0) b8 EMG5523-T50B: до V5.50 (ABPM.4) C0, V5.50 (ABSL.0) b8 EMG5723-T50K: до V5.50 (ABOM.5) C0 EMG6726-B10A: до V5.13 (ABNP.6) .C0 EX3510-B0: до V5.17 (ABUP.3) C0 EX5510-B0: до V5.15 (ABQX.3) C0 VMG3625-T50B: до V5.50 (ABPM.4) C0 VMG3925-B10B / B10C: до V5.13 (AAVF.16) C0 VMG3927-B50A_B60A: до V5.15 (ABMT.5) C0 VMG3927-B50B: до V5.13 (ABLY.6) C0 VMG3927-T50K: до V5.50 (ABOM.5) C0 VMG4005-B50B: до V5.13 (ABRL.5) C0 VMG4927-B50A: до V5.13 (ABLY.6) C0 VMG8623-T50B: до V5.50 (ABPM.4) C0 VMG8825-B50A_B60A: до V5.15 (ABMT.5) C0 VMG8825-Bx0B: до V5.15 (ABNY.5) C0 VMG8825-T50K: до V5.50 (ABOM.5) C0 VMG8924-B10D: до V5.13 (ABGQ.6) C0 XMG3927-B50A: до V5.15 (ABMT.5) C0

	XMG8825-B50A: до V5.15 (ABMT.5) C0 VMG1312-T20B: до V5.50 (ABSB.3) C0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 декабря 2020 г.
Дата обновления	19 декабря 2020 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	https://www.cybersecurity-help.cz/vdb/SB2020121920 https://www.zyxel.com/support/Zyxel-security-advisory-for-remote-code-execution-and-denial-of-service-vulnerabilities-of-CPE.shtml