НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200727.3| 27 июля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Некорректная аутентификация в устройствах ZTE R5300G4, R8500G4 и R5500G4

Идентификатор уязвимости	MITRE: CVE-2020-6871
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной обработкой запросов на аутентификацию в уязвимом программном обеспечении.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	R5300G4: V03.04.0020, V03.05.0040, V03.05.0043, V03.05.0044, V03.05.0045, V03.05.0046, V03.05.0047, V03.07.0100, V03.07.0108, V03.07.0200, V03.07.0300, V03.08.0100 R8500G4: V03.05.0020, V03.05.0400, V03.06.0100, V03.07.0101, V03.07.0103 R5500G4: V03.06.0100, V03.07.0100, V03.07.0200, V03.08.0100
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 июля 2020 г.
Дата обновления	24 июля 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	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1013203 https://nvd.nist.gov/vuln/detail/CVE-2020-6872