НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200316.1 | 16 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в ПО устройств компании Zyxel

Идентификатор уязвимости	MITRE: CVE-2020-9054
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с правами пользователя root в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой параметра username в файле weblogin.cgi.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Уязвимые устройства: NAS326 до v5.21 (AAZF.7) C0 NAS520 до v5.21 (AASZ.3) C0 NAS540 до v5.21 (AATB.4) C0 NAS542 до v5.21 (ABAG.4) C0 ATP100 до v4.35 (ABPS.3) C0 ATP200 до v4.35 (ABFW.3) C0 ATP500 до v4.35 (ABFU.3) C0 ATP800 до v4.35 (ABIQ.3) C0 USG20-VPN до v4.35 (ABAQ.3) C0 USG20W-VPN до v4.35 (ABAR.3) C0 USG40 до v4.35 (AALA.3) C0 USG40W до v4.35 (AALB.3) C0 USG60 до v4.35 (AAKY.3) C0 USG60W до v4.35 (AAKZ.3) C0 USG110 до v4.35 (AAPH.3) C0 USG210 до v4.35 (AAPI.3) C0 USG310 до v4.35 (AAPJ.3) C0 USG1100 до v4.35 (AAPK.3) C0 USG1900 до v4.35 (AAPL.3) C0

	USG2200 до v4.35 (ABAE.3) C0 VPN50 до v4.35 (ABHL.3) C0 VPN100 до v4.35 (ABFдо v.3) C0 VPN300 до v4.35 (ABFC.3) C0 VPN1000 до v4.35 (ABIP.3) C0 ZyWALL110 до v4.35 (AAAA.3) C0 ZyWALL310 до v4.35 (AAAB.3) C0 ZyWALL1100 до v4.35 (AAAC.3) C0 Уязвимые устройства, поддержка которых прекращена: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	4 марта 2020 г.
Дата обновления	6 марта 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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml https://krebsonsecurity.com/2020/02/zyxel-fixes-0day-in-network-storage-devices/ https://kb.cert.org/vuls/id/498544/