НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210927.1 | 27 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в SonicWall SMA 100 серии

Идентификатор уязвимости	MITRE: CVE-2021-20034
Идентификатор программной ошибки	CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить сброс конфигурации устройства до заводских настроек и вызвать отказ в обслуживании целевой системы посредством обхода введённых правил ограничения доступа и удаления файла конфигурации. Уязвимость обусловлена некорректными ограничениями доступа в интерфейсе управления SMA 100.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	SMA 100: 9.0.0.10-28sv, 10.2.0.2-20sv, 10.2.0.3-24sv, 10.2.0.5-d-29sv, 10.2.0.6-31sv, 10.2.0.7-34sv, 10.2.1.0-17sv
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	24 сентября 2021 г.
Дата обновления	24 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/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)	Отсутствует (N)
Влияние на целостность (I)	Низкое (L)
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/SB2021092406 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0021