НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200320.8 | 20 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании SSH-сервера в Mikrotik RouterOS

Идентификатор уязвимости	Отсутствует
Идентификатор программной ошибки	CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить атаку типа отказ в обслуживании SSH-сервера в Mikrotik RouterOS посредством направления вредоносных сетевых пакетов. Уязвимость обусловлена ошибками в управлении ресурсами в SSH-сервере.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	MikroTik RouterOS: 6.44, 6.44.1, 6.44.2, 6.44.3
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 марта 2020 г.
Дата обновления	19 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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)	Изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)

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.exploit-db.com/exploits/48228/