

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201105.3 | 5 ноября 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в ntopng

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	ntopng: 3.8, 3.8.1, 4.0
Дата выявления	2 ноября 2020 г.
Дата обновления	3 ноября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: N/A	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена неконтролируемым использованием внутренних ресурсов.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов)</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	7.5

MITRE: N/A	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной обработкой HTTP-запросов.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	9.8
---------------	---	-----

Ссылки на источники <https://www.cybersecurity-help.cz/vdb/SB2020110219>