НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200605.9 | 5 июня 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Node.js

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Node.js до v10.21.0 Node.js до v12.18.0 Node.js до v14.4.0
Дата выявления	2 июня 2020 г.
Дата обновления	2 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-11080	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки многочисленных сетевых пакетов HTTP/2 SETTINGS. Уязвимость обусловлена некорректным использованием выделенной памяти при обработке пакетов HTTP/2 SETTINGS. 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) Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2020-8174	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством передачи специально сформированных вредоносных данных. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке данных в функциях napi_get_value_string_latin1(), napi_get_value_string_utf8() и napi_get_value_string_utf16(). 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-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: обновить программное обеспечение.	9.8

Ссылки на источники	https://nodejs.org/en/blog/vulnerability/june-2020-security-releases/ https://www.cybersecurity-help.cz/vdb/SB2020060305