НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221116.6 | 16 ноября 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Node.js

Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	Node.js: 14.2.0 - 14.21.0, 18.1.0 - 18.12.0, 16.1.0 - 16.18.0, 18.4.0, 18.3.0, 17.9.0 - 17.9.1, 16.15.0 - 16.15.1, 14.19.0 - 14.19.3, 18.2.0, 18.0.0, 17.8.0, 17.7.0 - 17.7.2, 16.14.0 - 16.14.2, 17.6.0, 17.5.0, 17.4.0, 17.3.0 - 17.3.1, 16.13.0 - 16.13.2, 14.18.0 - 14.18.3, 17.2.0, 17.1.0, 17.0.0 - 17.0.1, 16.12.0, 16.11.0 - 16.11.1, 16.10.0, 16.9.0 - 16.9.1, 14.17.0 - 14.17.6, 16.8.0, 16.7.0, 16.6.0 - 16.6.2, 16.5.0, 16.4.0 - 16.4.2, 16.3.0, 16.2.0, 16.0.0, 15.14.0, 14.16.0 - 14.16.1, 15.13.0, 15.12.0, 15.11.0, 15.10.0, 15.9.0, 14.15.0 - 14.15.5, 15.8.0, 15.7.0, 15.6.0, 15.5.0 - 15.5.1, 15.4.0, 15.3.0, 15.2.0 - 15.2.1, 15.1.0, 15.0.0 - 15.0.1, 14.14.0, 14.13.0 - 14.13.1, 14.12.0, 14.11.0, 14.10.0 - 14.10.1, 14.9.0, 14.8.0, 14.7.0, 14.6.0, 14.5.0, 14.4.0, 14.3.0, 14.1.0, 14.0.0
Дата выявления	15 ноября 2022 г.
Дата обновления	15 ноября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-3602 CVE-2022-3786	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.	7.5

	CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	
MITRE: CVE-2022-43548	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в браузере клиента. Уязвимость обусловлена некорректной проверкой восьмеричного IP-адреса. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N CWE-350: Использование обратного разрешения DNS для принятия решений, связанных с безопасностью Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.5

Ссылки на источники	http://nodejs.org/en/blog/vulnerability/november-2022-security-releases/