НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200619.6 | 19 июня 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в компонентах ПО npm

Категория уязвимого продукта	Средства защиты информации
Уязвимое ПО	mosc 1.0.0 node-extend: 0.0.1, 0.0.2, 0.0.3, 0.0.4, 0.0.5, 0.0.6, 0.0.7, 0.0.8, 0.2.0 cd-messenger до v2.7.26
Дата выявления	12 июня 2020 г.
Дата обновления	12 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-7672 (mosc) CVE-2020-7673 (node-extend)	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные shell -команды в целевой системе посредством отправки специально сформированных вредоносных данных в уязвимое приложение. Уязвимость обусловлена некорректной проверкой входных данных и выполнением аргумента «A» из функции «extend» (A, B, as, isAargs), расположенной в «lib / exte.js», в функцией «eval». CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: на данный момент отсутствуют.	9.8

MITRE: CVE-2020-7675 (cd-messenger)	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные shell -команды в целевой системе посредством отправки специально сформированных вредоносных данных в уязвимое приложение. Уязвимость обусловлена некорректной проверкой входных данных в аргументе «color», выполняемом функцией «eval». CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: на данный момент отсутствуют.	9.8

Ссылки на источники	https://snyk.io/vuln/SNYK-JS-MOSC-571492 https://www.cybersecurity-help.cz/vdb/SB2020061111 https://snyk.io/vuln/SNYK-JS-NODEEXTEND-571491 https://www.cybersecurity-help.cz/vdb/SB2020061110 https://snyk.io/vuln/SNYK-JS-CDMESSENGER-571493 https://www.cybersecurity-help.cz/vdb/SB2020061205