НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200602.3| 2 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Несанкционированный доступ к траффику в EM-HTTP-Request

Идентификатор уязвимости	MITRE: CVE-2020-13482
Идентификатор программной ошибки	CWE-295: Некорректная проверка сертификатов
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить атаку «человек посередине». Уязвимость обусловлена недостаточной проверкой TLS сертификата в библиотеке eventmachine.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	EM-HTTP-Request v1.1.5
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	25 мая 2020 г.
Дата обновления	27 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)

Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Отсутствует
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://github.com/igrigorik/em-http-request/issues/339 https://www.cybersecurity-help.cz/vdb/SB2020060101