НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210322.1 | 22 марта 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Apache Velocity Engine

Идентификатор уязвимости	MITRE: CVE-2020-13936
Идентификатор программной ошибки	CWE-94: Некорректное управление генерированием кода (внедрение кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством изменения шаблона Velocity. Уязвимость обусловлена некорректной обработкой шаблонов Velocity.
Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Apache Velocity Engine: 1.1, 1.1-RC1, 1.1-RC2, 1.2, 1.2-RC1, 1.2-RC2, 1.2-RC3, 1.3, 1.3-RC1, 1.3.1, 1.3.1-RC1, 1.3.1-RC2, 1.4, 1.4-RC1, 1.5, 1.5-BETA1, 1.5-BETA2, 1.6, 1.6-beta1, 1.6-beta2, 1.6.1, 1.6.2, 1.6.3, 1.6.4, 1.7, 1.7-beta1, 2.0, 2.0-RC1, 2.0-RC2, 2.0-RC3, 2.0-RC4, 2.0-RC5, 2.0-RC6, 2.0-RC7, 2.0-RC8, 2.1, 2.1-RC1, 2.1-RC2, 2.2, 2.2-RC1, 2.2-RC2, 2.2-RC3, 2.2-RC4, 2.2-RC5, 2.3-RC1, 2.3-RC2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 марта 2021 г.
Дата обновления	16 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
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	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021031618 http://www.openwall.com/lists/oss-security/2021/03/10/1 https://lists.apache.org/thread.html/r01043f584cbd47959fabe18fff64de940f81a65024bb8dddbda31d9a%40%3Cuser.velocity.apache.org%3E https://lists.apache.org/thread.html/r01043f584cbd47959fabe18fff64de940f81a65024bb8dddbda31d9a@%3Cuser.velocity.apache.org%3E https://lists.apache.org/thread.html/r3ea4c4c908505b20a4c268330dfe7188b90c84dcf777728d02068ae6@%3Cannounce.apache.org%3E https://lists.apache.org/thread.html/rb042f3b0090e419cc9f5a3d32cf0baff283ccd6fcb1caea61915d6b6@%3Ccommits.velocity.apache.org%3E