НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220327.9 | 27 марта 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного PHP-кода в Symfony Twig

Идентификатор уязвимости	MITRE: CVE-2022-23614
Идентификатор программной ошибки	CWE-254: Уязвимости в безопасности ПО
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный PHP-код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректными ограничениями безопасности.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	Twig: 3.3.0 - 3.3.7, 2.0.0 - 3.3.7
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.
Дата выявления	24 марта 2022 г.
Дата обновления	24 марта 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/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)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации	Не изменяется (U)

уязвимости (S)	
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/SB2022032424 http://github.com/twigphp/Twig/commit/2eb33080558611201b55079d07ac88f207b466d5 http://github.com/twigphp/Twig/commit/22b9dc3c03ee66d7e21d9ed2ca76052b134cb9e9 http://github.com/twigphp/Twig/security/advisories/GHSA-5mv2-rx3q-4w2v http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OTN4273U4RHVIXED64T7DSMJ3VYTPRE7/ http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/I2PVV5DUTRUECTIHMTWRI5Z7DVNYQ2YO/ http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/PECHIY2XLWUH2WLCNPDGNFMPHPRPCEDZ/ http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SIGZCFSYLPP7UVJ4E4NLHSOQSKYNXSAD/