НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201125.11 | 25 ноября 2020

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в XStream

Идентификатор уязвимости	MITRE: CVE-2020-26217
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством обработки пользователем специально созданного вредоносного файла с помощью уязвимой библиотеки. Уязвимость обусловлена некорректной обработкой входных данных.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	XStream до v1.4.14
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 ноября 2020 г.
Дата обновления	17 ноября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.0 AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
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://x-stream.github.io/security.html#framework https://nvd.nist.gov/vuln/detail/CVE-2020-26217