НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ
VULN-20230323.4 | 23 марта 2023 г.
Уровень опасности: ВЫСОКИЙ
Наличие обновления: НЕТ

Множественные уязвимости в Convert To Pipeline

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Convert To Pipeline: 1.0
Дата выявления	22 марта 2023 г.
Дата обновления	22 марта 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-28676	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой источника HTTP запроса. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-352: Подделка межсайтового запроса (CSRF) Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.8

MITRE: CVE-2023-28677	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд) Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	7.5

Ссылки на источники	http://jenkins.io/security/advisory/2023-03-21/