

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221101.8 | 1 ноября 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Apache Batik XML

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Batik XML: 1.6.1 - 1.15
Дата выявления	30 октября 2022 г.
Дата обновления	30 октября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-42890	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный JavaScript код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N</p> <p>CWE-94: Некорректное управление генерированием кода (внедрение кода)</p> <p>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.</p>	7.5

MITRE: CVE-2022-41704	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного SVG-изображения. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N</p> <p>CWE-94: Некорректное управление генерированием кода (внедрение кода)</p> <p>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.</p>	7.5
--------------------------	---	-----

Ссылки на источники	<p>http://www.debian.org/security/2022/dsa-5264</p> <p>http://issues.apache.org/jira/browse/BATIK-1338</p>	
---------------------	---	--