НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200619.2 | 19 июня 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимоти в компоненте libexif ОС Ubuntu

Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимое ПО	Ubuntu 20.04 LTS: libexif12 до v0.6.21-6ubuntu0.3 Ubuntu 19.10: libexif12 до v0.6.21-5.1ubuntu0.5 Ubuntu 18.04 LTS: libexif12 до v0.6.21-4ubuntu0.5 Ubuntu 16.04 LTS: libexif12 до v0.6.21-2ubuntu0.5 Ubuntu 14.04 ESM: libexif12 до v0.6.21-1ubuntu1 + esm5 Ubuntu 12.04 ESM: libexif12 до v0.6.20-2ubuntu0.6
Дата выявления	16 июня 2020 г.
Дата обновления	16 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-13112	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным и вызвать отказ в обслуживании в целевой системе. Уязвимость обусловлена ошибкой граничного условия при обработке EXIF-тега MakerNote. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение.	9.1

MITRE: CVE-2020-0198	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных вредоносных данных в уязвимое приложение. Уязвимость обусловлена ошибкой переполнения целых чисел в функции exif_data_load_data_content () в файле exif-data.c. CVSSv3.0: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-190: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение.	8.0
MITRE: CVE-2020-13113	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена ошибкой разыменования нулевого указателя при обработке EXIF-тега MakerNote. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-476: Разыменование нулевого указателя Рекомендации по устранению: обновить программное обеспечение.	7.5
MITRE: CVE-2020-13114	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти при обработке данных EXIF-тега Canon MakerNote. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	https://usn.ubuntu.com/4396-1/ https://www.cybersecurity-help.cz/vdb/SB2020061704