НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190801.1 | 1 августа 2019 г.

Уровень опасности: КРИТИЧЕСКИЙ

Уязвимость программного модуля LibreLogo в ПО LibreOffice

Идентификатор уязвимости	MITRE: CVE-2019-9848
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного документа d формате .doc, .docx, .xls, .xlsx, .ppt, .pptx. Уязвимость обусловлена наличием механизмов в модуле LibreLogo, запускающих программные алгоритмы на языке «Python» при наведении курсора на вредоносный объект
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимые системы и программное обеспечение	LibreOffice до v6.2.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 июля 2019 г.
Дата обновления	31 июля 2019 г.
Оценка критичности уязвимости (CVSSv3)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Не требуется (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)

Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки	https://nvd.nist.gov/vuln/detail/CVE-2019-9848 https://insinuator.net/2019/07/libreoffice-a-python-interpreter-code-execution-vulnerability-cve-2019-9848/ https://www.securitylab.ru/news/500191.php https://www.libreoffice.org/download/download/