

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20190902.1 | 2 сентября 2019 г.
Уровень опасности: **КРИТИЧЕСКИЙ**
Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в LibreOffice

Идентификатор уязвимости	MITRE: CVE-2019-9850 CVE-2019-9851
Идентификатор программной ошибки	CWE-20: Некорректная проверка ввода
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе в результате открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной обработкой скриптов LibreLogo.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	LibreOffice до v6.2.6.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 августа 2019 г.
Дата обновления	28 августа 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:U/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)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)

Ссылки на источники

<https://usn.ubuntu.com/4102-1/>
<https://www.libreoffice.org/about-us/security/advisories/cve-2019-9850/>
<https://www.libreoffice.org/about-us/security/advisories/cve-2019-9851/>
<https://nvd.nist.gov/vuln/detail/CVE-2019-9850>
<https://nvd.nist.gov/vuln/detail/CVE-2019-9851>