НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210922.1 | 22 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Выполнение произвольных команд ОС в macOS

Идентификатор уязвимости	Не определен
Идентификатор программной ошибки	CWE-939: Некорректная авторизация в обработчике нестандартных схем URL
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды ОС в целевой системе посредством открытия пользователем специально созданного вредоносного файла формата inetloc. Уязвимость обусловлена некорректной проверкой входных данных в macOS Finder при обработке пользовательских URI (File:// или fIle://).
Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	macOS: 10.14 18A391, 10.14.1 18B75, 10.14.1 18B2107, 10.14.1 18B3094, 10.14.2 18C54, 10.14.3 18D42, 10.14.3 18D43, 10.14.3 18D109, 10.14.4 18E226, 10.14.4 18E227, 10.14.5 18F132, 10.14.6 18G84, 10.14.6 18G87, 10.14.6 18G95, 10.14.6 18G103, 10.14.6 18G1012, 10.14.6 18G2022, 10.14.6 18G3020, 10.14.6 18G4032, 10.14.6 18G5033, 10.14.6 18G6020, 10.14.6 18G6032, 10.14.6 18G6042, 10.14.6 18G7016, 10.14.6 18G8012, 10.14.6 18G8022, 10.14.6 18G9028, 10.14.6 18G9216, 10.14.6 18G9323, 10.15 19A583, 10.15 19A602, 10.15 19A603, 10.15.1 19B88, 10.15.2 19C57, 10.15.3 19D76, 10.15.4 19E266, 10.15.4 19E287, 10.15.5 19F96, 10.15.5 19F101, 10.15.6 19G73, 10.15.6 19G2021, 10.15.7 19H2, 10.15.7 19H4, 10.15.7 19H15, 10.15.7 19H114, 10.15.7 19H512, 10.15.7 19H524, 10.15.7 19H1030, 10.15.7 19H1217, 10.15.7 19H1323, 10.15.7 19H1417, 11.0 20A2411, 11.0.1 20B29, 11.0.1 20B50, 11.1 20C69, 11.2 20D64, 11.2.1

	20D74, 11.2.1 20D75, 11.2.2 20D80, 11.2.3 20D91, 11.3 20E232, 11.3.1 20E241, 11.4 20F71, 11.5 20G71, 11.5.1 20G80, 11.5.2 20G95, 11.6 20G165
Рекомендации по устранению	Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами
Дата выявления	22 сентября 2021 г.
Дата обновления	22 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021092205 https://ssd-disclosure.com/ssd-advisory-macos-finder-rce/