НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220204.1 | 4 февраля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Samba

Идентификатор уязвимости	MITRE: CVE-2021-44142
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия файлов в smbd. Уязвимость обусловлена ошибкой при анализе метаданных с расширенными атрибутами (EA, xattr). Уязвимость актуальная для Samba использующих модуль VFS vfs_fruit с параметрами по умолчанию (fruit:metadata=netatalk или fruit:resource=file).
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Samba до v4.13.17
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	31 января 2022 г.
Дата обновления	31 января 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)

Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2022013111 http://www.samba.org/samba/security/CVE-2021-44142.html