

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210331.2 | 31 марта 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Samba

Идентификатор уязвимости	MITRE: CVE-2020-27840
Идентификатор программной ошибки	CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код или вызвать отказ в обслуживании у целевой системы посредством отправки специально сформированного LDAP bind-запроса. Уязвимость обусловлена некорректной обработкой отличительных имен в LDAP bind-запросах.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Samba: 4.0.0-4.14.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	24 марта 2021 г.
Дата обновления	24 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021032411 https://www.samba.org/samba/security/CVE-2020-27840.html
---------------------	--