

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221228.20 | 28 декабря 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Samba

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Samba: 4.15.0 - 4.15.12
Дата выявления	15 декабря 2022 г.
Дата обновления	15 декабря 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-45141	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена ошибкой, которая заставляет сервер выдать зашифрованные данные.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-327: Использование скомпрометированного или ненадежного криптографического алгоритма</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	8.1

<p>MITRE: CVE-2022-38023 BDU: 2022-06830</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректно реализованной функции безопасности.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-254: Уязвимости в безопасности ПО</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.1</p>
<p>MITRE: CVE-2022-37966 BDU: 2022-06786</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе посредством проведения атаки типа «человек посередине». Уязвимость обусловлена некорректными ограничениями безопасности.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.1</p>

Ссылки на источники

- <https://bdu.fstec.ru/vul/2022-06786>
- <http://www.samba.org/samba/security/CVE-2022-45141.html>
- <https://bdu.fstec.ru/vul/2022-06830>
- <http://www.samba.org/samba/security/CVE-2022-37966.html>
- <http://www.samba.org/samba/security/CVE-2022-38023.html>