НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ
VULN-20211111.1 | 11 ноября 2021 г.
Уровень опасности: КРИТИЧЕСКИЙ
Наличие обновления: ЕСТЬ

Множественные уязвимости в Samba

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Samba: 3.0, 3.0.0, 3.0.1, 3.0.2, 3.0.2a, 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.0.7, 3.0.8, 3.0.9, 3.0.10, 3.0.11, 3.0.12, 3.0.13, 3.0.14, 3.0.14a, 3.0.15, 3.0.16, 3.0.17, 3.0.18, 3.0.19, 3.0.20, 3.0.20a, 3.0.20b, 3.0.21, 3.0.21a, 3.0.21b, 3.0.21c, 3.0.22, 3.0.23, 3.0.23a, 3.0.23b, 3.0.23c, 3.0.23d, 3.0.24, 3.0.25, 3.0.25a, 3.0.25b, 3.0.25c, 3.0.26, 3.0.26a, 3.0.27, 3.0.27a, 3.0.28, 3.0.28a, 3.0.29, 3.0.30, 3.0.31, 3.0.32, 3.0.33, 3.0.34, 3.0.35, 3.0.36, 3.0.37, 3.1, 3.1.0, 3.2, 3.2.0, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.2.7, 3.2.8, 3.2.9, 3.2.10, 3.2.11, 3.2.12, 3.2.13, 3.2.14, 3.2.15, 3.3, 3.3.0, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.3.6, 3.3.7, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12, 3.3.13, 3.3.14, 3.3.15, 3.3.16, 3.4, 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.4.9, 3.4.10, 3.4.11, 3.4.12, 3.4.13, 3.4.14, 3.4.15, 3.4.16, 3.4.17, 3.5, 3.5.0, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, 3.5.6, 3.5.7, 3.5.8, 3.5.9, 3.5.10, 3.5.11, 3.5.12, 3.5.13, 3.5.14, 3.5.15, 3.5.16, 3.5.17, 3.5.18, 3.5.19, 3.5.20, 3.5.21, 3.5.22, 3.6.0, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 3.6.11, 3.6.12, 3.6.13, 3.6.14, 3.6.15, 3.6.16, 3.6.17, 3.6.18, 3.6.19, 3.6.20, 3.6.21, 3.6.22, 3.6.23, 3.6.24, 3.6.25, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6, 4.0.7, 4.0.8, 4.0.9, 4.0.10, 4.0.11, 4.0.12, 4.0.13, 4.0.14, 4.0.15, 4.0.16, 4.0.17, 4.0.18, 4.0.19, 4.0.20, 4.0.21, 4.0.22, 4.0.23, 4.0.24, 4.0.25, 4.0.26, 4.1.0, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.1.8, 4.1.9, 4.1.10, 4.1.11, 4.1.12, 4.1.13, 4.1.14, 4.1.15, 4.1.16, 4.1.17, 4.1.18, 4.1.19, 4.1.20, 4.1.21, 4.1.22, 4.1.23, 4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 4.2.7, 4.2.8, 4.2.9, 4.2.10, 4.2.11, 4.2.12, 4.2.13, 4.2.14, 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.3.7, 4.3.8, 4.3.9, 4.3.10, 4.3.11,

	4.3.12, 4.3.13, 4.4.0, 4.4.0 rc4, 4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.4.10, 4.4.11, 4.4.12, 4.4.13, 4.4.14, 4.4.15, 4.4.16, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, 4.5.6, 4.5.7, 4.5.8, 4.5.9, 4.5.10, 4.5.11, 4.5.12, 4.5.13, 4.5.14, 4.5.15, 4.5.16, 4.6.0, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7, 4.6.8, 4.6.9, 4.6.10, 4.6.11, 4.6.12, 4.6.13, 4.6.14, 4.6.15, 4.6.16, 4.7.0, 4.7.1, 4.7.2, 4.7.3, 4.7.4, 4.7.5, 4.7.6, 4.7.7, 4.7.8, 4.7.9, 4.7.10, 4.7.11, 4.7.12, 4.8.0, 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7, 4.8.8, 4.8.9, 4.8.10, 4.8.11, 4.8.12, 4.9.0, 4.9.1, 4.9.2, 4.9.3, 4.9.4, 4.9.5, 4.9.6, 4.9.7, 4.9.8, 4.9.9, 4.9.10, 4.9.11, 4.9.12, 4.9.13, 4.9.14, 4.9.15, 4.9.16, 4.9.17, 4.9.18, 4.10.0, 4.10.1, 4.10.2, 4.10.3, 4.10.4, 4.10.5, 4.10.6, 4.10.7, 4.10.8, 4.10.9, 4.10.10, 4.10.11, 4.10.12, 4.10.13, 4.10.14, 4.10.15, 4.10.16, 4.10.17, 4.10.18, 4.11.0, 4.11.1, 4.11.2, 4.11.3, 4.11.4, 4.11.5, 4.11.6, 4.11.7, 4.11.8, 4.11.9, 4.11.10, 4.11.11, 4.11.12, 4.11.13, 4.11.14, 4.11.15, 4.11.16, 4.11.17, 4.12.0, 4.12.1, 4.12.2, 4.12.3, 4.12.4, 4.12.5, 4.12.6, 4.12.7, 4.12.8, 4.12.9, 4.12.10, 4.12.11, 4.12.12, 4.12.13, 4.12.14, 4.12.15, 4.13.0, 4.13.1, 4.13.2, 4.13.3, 4.13.4, 4.13.5, 4.13.6, 4.13.7, 4.13.8, 4.13.9, 4.13.10, 4.13.11, 4.13.12, 4.13.13, 4.14.0, 4.14.1, 4.14.2, 4.14.3, 4.14.4, 4.14.5, 4.14.6, 4.14.7, 4.14.8, 4.14.9, 4.15.0, 4.15.1
Дата выявления	10 ноября 2021 г.
Дата обновления	10 ноября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2016-2124	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к ограниченным функциям в целевой системе посредством перехвата пароля в виде открытого текста. Уязвимость обусловлена некорректной реализацией протокола SMB1. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2020-25717	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена возможностью создания учетных записей компьютеров с повышенными привилегиями в системе. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение	8.1
MITRE: CVE-2020-25718	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в Samba Active Directory Domain Controller. CVSSv3.0: AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2020-25722	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение	8.8

MITRE: CVE-2021-3738	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии и вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена ошибкой использования после освобождения. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение	7.6

Ссылки на источники	http://www.samba.org/samba/security/CVE-2020-25722.html http://www.samba.org/samba/security/CVE-2016-2124.html https://www.cybersecurity-help.cz/vdb/SB2021111008 http://www.samba.org/samba/security/CVE-2020-25717.html http://www.samba.org/samba/security/CVE-2021-3738.html http://www.samba.org/samba/security/CVE-2020-25718.html