НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211124.5 | 24 ноября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Salt

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Salt: 3003, 3003.1, 3003.2
Дата выявления	23 ноября 2021 г.
Дата обновления	23 ноября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-31607	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в модуле snapper. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд) Рекомендации по устранению: обновить программное обеспечение	7.8

MITRE: CVE-2021-25283	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных. 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-94: Некорректное управление генерированием кода (внедрение кода) Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-25281	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить несанкционированный доступ к ограниченным функциям посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректными ограничениями доступа. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:F/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение	8.1
MITRE: CVE-2021-3197	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных. 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-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: обновить программное обеспечение	9.8
MITRE: CVE-2021-3148	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных. 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-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд) Рекомендации по устранению: обновить программное обеспечение	8.1

MITRE: CVE-2021-3144	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации посредством использования истекшего токена eauth. Уязвимость обусловлена некорректной обработкой запросов аутентификации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-287: Некорректная аутентификация Рекомендации по устранению: обновить программное обеспечение	9.1
MITRE: CVE-2020-28243	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии и создавать файлы в каталогах 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:N/E:P/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение	8.1

Ссылки на источники	http://github.com/saltstack/salt/releases http://sec.stealthcopter.com/saltstack-snapper-minion-privledge-escaltion/ http://github.com/saltstack/salt/commit/43e4ac985a2fc5f0d596c9fc6bc700b0d1af5344 https://www.cybersecurity-help.cz/vdb/SB2021112302 http://saltproject.io/security_announcements/active-saltstack-cve-release-2021-feb-25/ http://www.saltstack.com/blog/active-saltstack-cve-announced-2021-jan-21/ http://bugzilla.redhat.com/show_bug.cgi?id=1953065 http://saltproject.io/security_announcements/salt-security-advisory-2021-sep-02/