НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200506.5| 6 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в ОС Arch Linux

Идентификатор уязвимости	MITRE: CVE-2020-11651
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Уязвимость позволяет удаленному злоумышленнику выполнять произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой аутентификации системой управления Salt Master в классе ClearFuncs при вызове методов, которые используются для извлечения пользовательских токенов и запуска произвольных команд.
Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимое ПО	SaltStack Salt до v2019.2.4, v3000 до v3000.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 мая 2020 г.
Дата обновления	5 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
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)	Низкое (N)
Степень зрелости доступных средств эксплуатации	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://security.archlinux.org/CVE-2020-11651 https://nvd.nist.gov/vuln/detail/CVE-2020-11651 https://www.cybersecurity-help.cz/vdb/SB2020050506