НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220526.10 | 26 мая 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Nomad

Идентификатор уязвимости	MITRE: CVE-2022-30324
Идентификатор программной ошибки	CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	Nomad: 1.1.0 - 1.1.13, 1.2.0 - 1.2.7, 1.1.0 - 1.3.0
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.
Дата выявления	23 мая 2022 г.
Дата обновления	23 мая 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C
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	Не изменяется (U)

уязвимости (S)	
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	http://github.com/hashicorp/nomad/releases/tag/v1.3.1 http://github.com/hashicorp/nomad/releases/tag/v1.1.14 http://github.com/hashicorp/nomad/releases/tag/v1.2.8