НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200522.13| 22 мая 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco Prime Network Registrar

Идентификатор уязвимости	MITRE: CVE-2020-3272
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально созданного вредоносного DHCP-запроса на уязвимое устройство. Уязвимость обусловлена некорректной проверкой входящего DHCP трафика.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Cisco Prime Network Registrar: v8.3.0, v9.0, 9.1, v10.0, v10.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	20 мая 2020 г.
Дата обновления	20 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Удаленный (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)	Отсутствует (N)

Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020052118 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpnr-dhcp-dos-BkEZfhLP