НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200207.2 | 7 февраля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Discovery Protocol

Идентификатор уязвимости	MITRE: CVE-2020-3110 CVE-2020-3111 CVE-2020-3118 CVE-2020-3119 Cisco: cisco-sa-20200205-ipcameras-rce-dos cisco-sa-20200205-voip-phones-rce-dos cisco-sa-20200205-iosxr-cdp-rce cisco-sa-20200205-nxos-cdp-rce
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных CWE-134: Использование форматной строки, контролируемой извне CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код на целевом устройстве посредством отправки вредоносного пакета Cisco Discovery Protocol. Уязвимость обусловлена некорректной проверкой при обработке сообщений.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco Video Surveillance 8000 Series IP Cameras до v1.0.7 IP Conference Phone v7832 IP Conference Phone v8832 IP Phone v6821, v6841, v6851, v6861, v6871 IP Phone v7811, v7821, v7841, v7861 Desktop Phones IP Phone v8811, v8841, v8851, v8861, v8845, v8865 Desktop Phones Unified IP Conference Phone v8831 Wireless IP Phone v8821, v8821-EX ASR 9000 Series Aggregation Services Routers Carrier Routing System (CRS)

	IOS XRv 9000 Router Network Convergence System (NCS) 540 Series Routers NCS 560 Series Routers NCS 1000 Series Routers NCS 5000 Series Routers NCS 5500 Series Routers NCS 6000 Series Routers Nexus 3000 Series Switches Nexus 5500 Platform Switches Nexus 5600 Platform Switches Nexus 6000 Series Switches Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode Nexus 9000 Series Switches in standalone NX-OS mode UCS 6200 Series Fabric Interconnects UCS 6300 Series Fabric Interconnects UCS 6400 Series Fabric Interconnects
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 февраля 2020 г.
Дата обновления	5 февраля 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Смежная сеть (A)
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)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)

Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-ipcameras-rce-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-voip-phones-rce-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-nxos-cdp-rce https://www.armis.com/cdpwn/