НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210709.2 | 9 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Business Process Automation

Идентификатор уязвимости	MITRE: CVE-2021-1574 CVE-2021-1576
Идентификатор программной ошибки	CWE-798: Использование жестко закодированных учетных данных
Описание уязвимости	Эксплуатация уязвимостей позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированных HTTP-сообщений. Уязвимости обусловлены некорректными настройками авторизации для команд управления и настройками доступа к журналам действий.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Cisco Business Process Automation до v3.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 июля 2021 г.
Дата обновления	8 июля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/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)	Низкий (L)
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)	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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bpa-priv-esc-dgubwbH4