НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220209.2 | 9 февраля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Выполнение произвольного кода в ПО F5 Networks

Идентификатор уязвимости	MITRE: CVE-2020-10878
Идентификатор программной ошибки	CWE-190: Целочисленное переполнение или циклический возврат
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	BIG-IQ Centralized Management: до 8.1.0 F5OS: до 1.3.1
Рекомендации по устранению	Ограничить доступ к уязвимому продукту средствами межсетевого экранирования другими административными мерами
Дата выявления	7 февраля 2022 г.
Дата обновления	7 февраля 2022 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	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	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2022020717 https://www.cybersecurity-help.cz/vdb/SB2022020719 http://support.f5.com/csp/article/K40508224