НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221005.1 | 5 октября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Dell EMC AppSync

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Dell EMC AppSync: до 4.4.1.0
Дата выявления	26 сентября 2022 г.
Дата обновления	26 сентября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2019-12900	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-787: Запись за границами буфера 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.	9.8

MITRE: CVE-2021-33503	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректной проверкой ввода. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) 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.	7.5

Ссылки на источники	http://www.dell.com/support/kbdoc/fr-fr/printview/000199436/10/en (Данный сайт недоступен с IP-адресов Российской Федерации)