НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221005.7 | 5 октября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Dell Support Assist Enterprise

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Dell Support Assist Enterprise: до 5.00.06
Дата выявления	23 сентября 2022 г.
Дата обновления	23 сентября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-44228	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H CWE-94: Некорректное управление генерированием кода (внедрение кода) 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.	10.0

MITRE: CVE-2021-45046	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H CWE-94: Некорректное управление генерированием кода (внедрение кода) 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.	9.0
MITRE: CVE-2021-45105	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена зацикливанием внутри класса. CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-835: Бесконечный цикл (зацикливание) 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.	5.9

Ссылки на источники	http://www.dell.com/support/kbdoc/nl-nl/000194724/dsa-2021-283-dell-emc-support-assist-enterprise-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228-cve-2021-45046-cve-2021-45105 (Данный сайт недоступен с IP-адресов Российской Федерации)