НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221005.10 | 5 октября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Dell Elastic Cloud Storage (ECS)

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	EMC ECS: до 3.7.0.2
Дата выявления	26 сентября 2022 г.
Дата обновления	26 сентября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-21449 CVE-2022-21476 CVE-2022-22719	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной проверкой входных данных. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CWE-20: Некорректная проверка входных данных 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

MITRE: CVE-2020-15862	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с привилегиями «root». Уязвимость обусловлена небезопасными разрешениями для Net-snmp. CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-732: Некорректные разрешения для критически важных 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.	7.8
MITRE: CVE-2021-4156	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством открытия пользователем специально сформированных данных. Уязвимость обусловлена граничным условием в функции. CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H CWE-125: Чтение за пределами 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.	8.1
MITRE: CVE-2022-0778	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена зацикливание внутри функции. CVSS:3.1/AV:N/AC:L/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.	7.5

MITRE: CVE-2018-25032 CVE-2020-19131	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-119: Выполнение операций за пределами буфера памяти 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
MITRE: CVE-2022-25235	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:U/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.	9.8
MITRE: CVE-2020-35524	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного TIFF-изображения. Уязвимость обусловлена ошибкой границ памяти. CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-119: Выполнение операций за пределами буфера памяти 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.	7.8

MITRE: CVE-2020-35523	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена целочисленным переполнением. CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-190: Целочисленное переполнение или циклический возврат 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.	7.8
MITRE: CVE-2019-17546 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного RGBA-изображения. Уязвимость обусловлена целочисленным переполнением. CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-190: Целочисленное переполнение или циклический возврат 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.	8.8
MITRE: CVE-2017-17095	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена ошибкой границ памяти. CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-122: Переполнение буфера в динамической памяти 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.	8.8

MITRE: CVE-2018-16301	Эксплуатация уязвимости позволяет локальному злоумышленнику вызвать отказ в обслуживании целевой системы посредством открытия пользователем специально сформированных данных. Уязвимость обусловлена граничным условием в функции. CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-125: Чтение за пределами 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.	7.8
MITRE: CVE-2022-0391	Эксплуатация уязвимости позволяет удаленному злоумышленнику посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N CWE-93: Некорректная нейтрализация последовательностей символов CRLF (внедрение символов CRLF) 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
MITRE: CVE-2022-23943	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. 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-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-23852 CVE-2022-23990 CVE-2022-25315	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-190: Целочисленное переполнение или циклический возврат 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-2021-46143	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-190: Целочисленное переполнение или циклический возврат 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.	8.1
MITRE: CVE-2021-45960	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректным потреблением внутренних ресурсов. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/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.	8.8

MITRE: CVE-2022-24407	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных уязвимого приложения посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-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.	8.8
MITRE: CVE-2022-22721	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена целочисленным переполнением. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H CWE-190: Целочисленное переполнение или циклический возврат 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.	9.1
MITRE: CVE-2022-22720	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректным закрытием входящего соединения. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-444: Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы) 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-2021-44790 CVE-2022-23218 CVE-2022-23219	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. 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-119: Выполнение операций за пределами буфера памяти 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-2021-44224	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить SSRF-атаку посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена подделкой запросов со стороны сервера. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H CWE-918: Подделка запроса со стороны сервера 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.	8.2
MITRE: CVE-2021-45417	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-122: Переполнение буфера в динамической памяти 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.	7.8

MITRE: CVE-2021-3999	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-193: Ошибка смещения на единицу 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.	7.8
MITRE: CVE-2022-25314	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-190: Целочисленное переполнение или циклический возврат 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
MITRE: CVE-2022-25236	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-20: Некорректная проверка входных данных 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

Ссылки на источники	http://www.dell.com/support/kbdoc/nl-nl/000200286/dsa-2022-157-dell-elastic-cloud-storage-ecs-security-update-for-multiple-third-party-component-vulnerabilities (Данный сайт недоступен с IP-адресов Российской Федерации)