НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220331.5 | 31 марта 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Western Digital My Cloud OS 5

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	My Cloud PR2100: Все версии My Cloud PR4100: Все версии My Cloud EX4100: Все версии My Cloud EX2 Ultra: Все версии My Cloud Mirror Gen 2: Все версии My Cloud DL2100: Все версии My Cloud DL4100: Все версии My Cloud EX2100: Все версии My Cloud: Все версии WD Cloud: Все версии My Cloud Home: Все версии My Cloud OS 5: до 5.19.117, 7.16-220
Дата выявления	25 марта 2022 г.
Дата обновления	25 марта 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS

MITRE: CVE-2022-0194 CVE-2022-23122 CVE-2022-23125	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке 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-2022-23121	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной обработкой исключений. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-755: Некорректная обработка исключений 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-2022-23123 CVE-2022-23124	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольный файлы в целевой системе. Уязвимость обусловлена граничным условием. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C 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.	7.5

MITRE: CVE-2022-22995	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить и запустить произвольный файл на сервере. Уязвимость обусловлена некорректной проверкой файла во время загрузки. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-434: Отсутствие ограничений на загрузку файлов небезопасного типа 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.westerndigital.com/support/product-security/wdc-22005-netatalk-security-vulnerabilities