НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230301.1 | 1 марта 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Dell EGW-5200

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	EGW-5200: до 1.06.10 2V4
Дата выявления	23 февраля 2023 г.
Дата обновления	23 февраля 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-26845	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена некорректной аутентификацией. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N CWE-287: Некорректная аутентификация 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.	8.7

MITRE: CVE-2022-27497	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой разыменования указателя NULL. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H CWE-476: Разыменование нулевого указателя 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.	8.6
MITRE: CVE-2022-29893	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена некорректной аутентификацией. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N CWE-287: Некорректная аутентификация 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

Ссылки на источники	http://www.dell.com/support/kbdoc/nl-nl/000209731/dsa-2023-042-dell-networking-security-update-for-a-third-party-bios-vulnerability