НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220127.2 | 27 января 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в RLC-410W

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	RLC-410W: 3.0.0.136_20121102
Дата выявления	27 января 2022 г.
Дата обновления	27 января 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-40419	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректным обновлением прошивки. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-489: Присутствует код отладки Рекомендации по устранению: обновить программное обеспечение	10.0

MITRE: CVE-2022-21796	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение	9.3
MITRE: CVE-2021-40406	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректным использованием ресурсов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2022-21134	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально сформированного запроса. Уязвимость обусловлена некорректным управлением сигнатурами в функции. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-347: Некорректная проверка криптографической подписи Рекомендации по устранению: обновить программное обеспечение	8.3
MITRE: CVE-2021-40407 CVE-2021-40408 CVE-2021-40409 CVE-2021-40410 CVE-2021-40411 CVE-2021-40412	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: обновить программное обеспечение	9.1

MITRE: CVE-2021-40405	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректными ограничениями доступа. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение	7.7
MITRE: CVE-2022-21217	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение	9.1
MITRE: CVE-2022-21801	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-190: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение	8.6

Ссылки на источники	http://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1428 http://www.talosintelligence.com/vulnerability_reports/TALOS-2022-1451 http://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1422 http://www.talosintelligence.com/vulnerability_reports/TALOS-2022-1447 http://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1423 http://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1424 http://www.talosintelligence.com/vulnerability_reports/TALOS-2022-1450

	http://www.talosintelligence.com/vulnerability_reports/TALOS-2022-1445 https://www.cybersecurity-help.cz/vdb/SB2022012706