# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220419.27 | 19 апреля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

## Множественные уязвимости в Red Lion DA50N

| | |
|---|---|
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | DA50N: все версии |
| Дата выявления | 19 апреля 2022 г. |
| Дата обновления | 19 апреля 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE: CVE-2022-26516 | Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить НСД к целевой системе посредством отправки специально созданного вредоносного файла обновления. Уязвимость обусловлена некорректной авторизацией.<br>CVSSv3.0: AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H/E:U/RL:U/RC:C<br>CWE-345: Некорректная проверка достоверности данных<br>Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами. | 8.4 |

| | | |
|---|---|---|
| MITRE:<br>CVE-2022-1039 | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена слабой парольной политикой.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:U/RC:C<br>CWE-521: Недостаточные требования к паролю<br>Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами. | 9.6 |

| | |
|---|---|
| Ссылки на источники | http://ics-cert.us-cert.gov/advisories/icsa-22-104-03 |