# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211111.4 | 11 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Множественные уязвимости в Zyxel ZyWALL VPN2S

| | |
|---|---|
| Категория уязвимого продукта | Средства защиты информации |
| Уязвимый продукт | ZyWALL VPN2S: 1.12 |
| Дата выявления | 4 октября 2021 г. |
| Дата обновления | 4 октября 2021 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE: CVE-2021-35027 | Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольные файлы в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C<br>CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога)<br>Рекомендации по устранению: обновить программное обеспечение | 7.5 |

| | | |
|---|---|---|
| MITRE: CVE-2021-35028 | Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.<br>CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C<br>CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)<br>Рекомендации по устранению: обновить программное обеспечение | 7.8 |

| | |
|---|---|
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2021100401<br>http://www.zyxel.com/support/Zyxel_security_advisory_for_directory_traversal_and_command_injection_vulnerabilities_of_VPN2S_Firewall.shtml |