# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200131.1 | 31 января 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Удаленное выполнение команд в ПО rConfig

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2019-19509 |
| Идентификатор программной ошибки | CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить системные команды в целевой системе посредством отправки специально сформированных GET-запросов. Уязвимость обусловлена некорректной обработкой HTTP-запросов в файле ajaxArchiveFiles.php. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимое ПО | rConfig 3.9.3 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 7 ноября 2019 г. |
| Дата обновления | 30 января 2020 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Низкий (L) |
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации уязвимости (S) | Не изменяется (U) |
| Влияние на конфиденциальность (C) | Высокое (H) |

| | |
|---|---|
| Влияние на целостность (I) | Высокое (H) |
| Влияние на доступность (A) | Высокое (H) |
| Степень зрелости доступных средств эксплуатации (E) | Наличие не подтверждено (U) |
| Наличие средств устранения уязвимости (RL) | Официальное решение (O) |
| Достоверность сведений об уязвимости (RC) | Сведения подтверждены (C) |
| Ссылки на источники | https://packetstormsecurity.com/files/156146/rConfig-3.9.3-Remote-Code-Execution.html |