Выпущены Roundcube 1.6.21 и 1.7.6

9 ноября 2026 года опубликованы обновления безопасности Roundcube Webmail 1.6.21 и 1.7.6 для веток 1.6 LTS и 1.7. В обеих версиях исправлены недавно обнаруженные уязвимости.

Исправления безопасности

- Устранено открытое перенаправление при восстановлении после ошибки IMAP во время получения вложения. Об уязвимости сообщил Santhoshkumar S.
- Заголовок `Received:` теперь включает только доверенное имя хоста и IP-адрес, переданный доверенным прокси.
- Исправлена возможность выполнять некоторые разрушительные действия ManageSieve через межсайтовые GET-запросы.
- Устранено внедрение кода Sieve через оператор правила.
- Устранено внедрение кода Sieve через модификаторы `set` и `include`.
- Исправлена функция `resolve_url()`, игнорировавшая настройку доверенного хоста.
- Устранено внедрение почтовых заголовков через тему уведомления о прочтении (MDN).
- Устранено внедрение HTTP-запросов через сервер проверки орфографии ATD.

Об этих семи проблемах сообщили Squirt1e, Atum, N0b0dy и Gh0u1L5.

- Устранено внедрение команд IMAP через символы CRLF в параметре `_uid` при включённом `messages_cache`. Об уязвимости сообщил dexx-tech.
- Исправлен обход защиты от SSRF в CSS-прокси через домены `nip.io` и `sslip.io` из-за неполной проверки `is_local_url()`. Об уязвимости сообщил blacksw0rd.
- Устранён обход проверки CSRF для POST-запросов, содержащих только файлы.
- Исправлен обход ограничений `disabled_actions` путём замены дефиса на подчёркивание в имени действия.

Об этих двух проблемах сообщил skad00sh.

- Устранён обход проверки CSRF для команд очистки почты `purge` и `expunge`. Об уязвимости сообщил threalwinky.
- Исправлена передача потенциально опасного содержимого вложений в ImageMagick при преобразовании формата изображений. Об уязвимости сообщил José Luis Sánchez Pérez из Cybersecurity Blue & Red Team.
- Устранён бесконечный цикл с потреблением CPU и возможностью отказа в обслуживании в `rcube_session::unserialize()` при обработке токена с отрицательной длиной. Об уязвимости сообщил Guang.
- Исправлен обход SSRF-фильтра `is_local_url()` через адреса 6to4 из диапазона `2002::/16`. Об уязвимости сообщил wyx98765.

- Усилена проверка вводимого адреса IMAP-сервера. Об уязвимости сообщил Mohamed Elgzouli.

Обновление и поддержка ветки 1.6

Разработчики настоятельно рекомендуют обновить все рабочие установки Roundcube 1.6.x и 1.7.x до новых версий.

Ветке 1.6 уже четыре года, а перенос исправлений безопасности становится всё более трудоёмким и подверженным ошибкам. Разработчики предупреждают о скором прекращении её поддержки и рекомендуют запланировать переход на ветку 1.7. Точная дата завершения поддержки в анонсе не указана.

Полные списки изменений доступны на страницах выпусков Roundcube 1.6.21 и Roundcube 1.7.6.