Выпущены Roundcube 1.6.18 и 1.7.3

Выпущены Roundcube 1.6.18 и 1.7.3

Опубликованы обновления безопасности Roundcube Webmail 1.6.18 и 1.7.3. В обеих версиях исправлены недавно обнаруженные уязвимости.

Исправления безопасности

- Добавлена базовая проверка содержимого, передаваемого через CSS-прокси.
- Исправлен обход защиты от SSRF с помощью URL-адресов из локальных сетей `100.64.0.0/10` и `fe80::/10`. Об уязвимости сообщил Дмитрий Иваненко.
- Исправлен обход SSRF-фильтра с помощью различных вариантов имён хостов `nip.io` и `sslip.io`, позволявших обойти проверку `is_local_url()`. Об уязвимости сообщил Милан Хоппе.
- Исправлен обход блокировки удалённого содержимого с помощью незакрытого `url()` в атрибуте FuncIRI. Об уязвимости сообщил Милан Хоппе.
- Исправлена инъекция в LDAP-фильтр через неэкранированные подстановки %u, %fu и %d в `search_filter`. Об уязвимости сообщил Милан Хоппе.
- Исправлена возможность внедрения произвольного Sieve-скрипта через имя правила фильтра в обход `managesieve_disabled_actions`. Об уязвимости сообщил Милан Хоппе.
- Исправлена возможность удалённого выполнения кода через драйвер `cmd_learn` плагина `markasjunk`. Об уязвимости сообщил nept1337.
- Исправлена инъекция IMAP-команд через поиск почты и рассинхронизацию счётчика байтов `LITERAL+`. Об уязвимости сообщил Зак Хэнли из Horizon3.ai.
- Исправлена утечка токена аутентификации на подконтрольный пользователю хост в драйвере `modoboa` плагина `password`. Об уязвимости сообщил meifukun.
- Исправлена хранимая XSS-уязвимость в действии «Добавить в адресную книгу». Об уязвимости сообщил Паулос Йибело из pwn.ai.
- Исправлен обход очистки HTML и CSS с помощью атрибута by элемента SVG `animate`. Об уязвимости сообщил vectrain.

Полный список изменений приведён на страницах выпусков Roundcube 1.6.18 и Roundcube 1.7.3.

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