Выпущены Roundcube 1.6.19 и 1.7.4

Опубликованы обновления безопасности Roundcube Webmail 1.6.19 и 1.7.4 для веток 1.6 LTS и 1.7. В обеих версиях исправлены недавно обнаруженные уязвимости.

Исправления безопасности

- Исправлена возможность скрытого внедрения CSS-деклараций из-за вывода незакодированного символа амперсанда. Об уязвимости сообщил Зак Хэнли из Horizon3.ai.
- Исправлена инъекция CSS-свойств через атрибут `background` элемента body. Об уязвимости сообщил zenithhostingevan.
- Исправлена инъекция почтовых заголовков через одиночный символ возврата каретки (CR) в поле темы письма. Об уязвимости сообщил CVE-Hunter-Leo.
- Исправлена инъекция почтовых заголовков через escape-последовательность `\r` в стиле C в отображаемом имени получателя. Об уязвимости сообщил dogeshark.
- Исправлена инъекция почтовых заголовков через поле организации в профиле отправителя. Об уязвимости сообщил dogeshark.
- Исправлена хранимая XSS-уязвимость, не требующая действий пользователя, через внедрение MIME-тега TNEF в URL вложения. Об уязвимости сообщил nakko.
- Исправлена XSS-уязвимость в HTML-редакторе при обработке содержимого части письма с типом `text/enriched`. Об уязвимости сообщил Джошуа Роджерс.
- Исправлена возможность добавлять и удалять контакты в группах другого пользователя в адресной книге на базе SQL. Об уязвимости сообщил Джошуа Роджерс.
- Исправлен обход проверки `is_local_url()` с помощью полного доменного имени (FQDN) с точкой в конце в URL таблицы стилей. Об уязвимости сообщил nept1337.
- Исправлен обход блокировки удалённого содержимого с помощью escape-последовательностей CSS в атрибутах FuncIRI. Об уязвимости сообщил Вахаб Хадир.
- Исправлен обход блокировки удалённого содержимого через анимацию атрибута `src` средствами SVG SMIL.
- Исправлен обход защиты от SSRF в CSS-прокси Roundcube с помощью шестнадцатеричной записи IPv4-адресов, представленных в формате IPv6. Об уязвимости сообщили faceless0x7 и Хариш Аннависами.

Полный список изменений приведён на страницах выпусков Roundcube 1.6.19 и Roundcube 1.7.4.

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