В браузере Firefox, почтовом клиенте Thunderbird и их корпоративных версиях (ESR) компании Mozilla были обнаружены многочисленные недостатки в системе безопасности. Наиболее серьезные проблемы могут позволить злоумышленникам получить полный контроль над устройством, запустив вредоносный код без разрешения пользователя.

Эти уязвимости могут позволить хакерам устанавливать программы, красть или удалять данные, а также создавать новые учетные записи с полным доступом – особенно опасно, если у пользователя есть права администратора. Пользователи с ограниченным доступом могут подвергаться меньшему риску, но уязвимости все равно представляют угрозу.

К затронутым версиям относятся:

- Firefox версий до 138
- Firefox ESR версий до 115.23 и 128.10
- Thunderbird версий до 138 и ESR 128.10.

Хотя пока не известно ни одной атаки, использующей эти проблемы, пользователям и организациям настоятельно рекомендуется немедленно обновить свое программное обеспечение.

Проблемы включают в себя ошибки, влияющие на работу с памятью, позволяющие обойти функции безопасности, а также скрыть вредоносные загрузки или расширить доступ злоумышленников. Большинство из этих проблем уже исправлено в последних версиях программного обеспечения.

В зоне повышенного риска находятся государственные и крупные предприятия США.