# Рекомендации по безопасности Mozilla Foundation

| | |
|---|---|
| Критический | Уязвимость может быть использована для запуска злоумышленного кода и установки программного обеспечения, не требуя никакого взаимодействия с пользователем, кроме обычного просмотра. |
| Высокий | Уязвимость можно использовать для сбора конфиденциальных данных с сайтов в других окнах или для внедрения данных или кода на эти сайты, требуя не более чем обычных действий при просмотре. |
| Умеренный | Уязвимости, которые в противном случае были бы высокими или критическими, за исключением того, что они работают только в необычных конфигурациях, отличных от стандартных, или требуют от пользователя выполнения сложных и/или маловероятных действий. |
| Низкий | Незначительные уязвимости безопасности, такие как атаки типа «отказ в обслуживании», незначительные утечки данных или подделки. (Необнаружимые подделки знаков SSL будут иметь высокий уровень воздействия, поскольку они обычно используются для кражи конфиденциальных данных, предназначенных для других сайтов.) |

https://www.mozilla.org/en-US/security/advisories/

From:
https://wwoss.ru/ - **worldwide open-source software**

Permanent link:
**https://wwoss.ru/doku.php?id=software:development:web:docs:web:security:advisories:advisories**

Last update: **2023/08/30 13:17**