НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

# Эксплуатация уязвимости в OpenSSL

ALRT-20220317.1 | 17 марта 2022 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

| | |
|---|---|
| Уязвимое программное обеспечение | OpenSSL |
| Актуальность угрозы | По настоящее время |
| Описание | НКЦКИ предупреждает об актуальной угрозе проведения компьютерных атак, связанных с эксплуатацией уязвимости CVE-2022-0778 в OpenSSL.<br><br>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать ошибку типа «отказ в обслуживании» в целевой системе посредством отправки специально сформированных данных. Уязвимость присутствует в версиях OpenSSL: 3.0.0 - 3.0.1, 1.1.1 - 1.1.1m, 1.0 - 3.0.1.<br><br>Уязвимость представляет опасность в тех случаях, когда происходит обработка пользовательских сертификатов или приватных ключей, например:<br><br>- При подключениях по ssh/VPN к сервисам, использующим OpenSSL<br><br>- В случаях, когда со стороны пользователя есть возможность загрузить для обработки сертификат или ключ (т.е. компьютерным атакам могут быть подвержены удостоверяющие центры, принимающие запросы на выдачу сертификатов)<br><br>Производителем программного обеспечения оперативно было выпущено исправление указанной уязвимости. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.<br><br>Напоминаем, что в случае, если эксплуатация уязвимости повлекла компьютерный инцидент на объекте критической информационной инфраструктуры Российской Федерации, то его владелец (субъект КИИ) в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ обязан уведомить об этом НКЦКИ. |