

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Уязвимость нулевого дня в CMS Bitrix

ALRT-20220303.2 | 3 марта 2022 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE



| | |
|----------------------------------|---|
| Уязвимое программное обеспечение | CMS Bitrix |
| Актуальность угрозы | По настоящее время |
| Описание угрозы | <p>По каналам Национального координационного центра по компьютерным инцидентам получены сведения о ранее неизвестной критической уязвимости в CMS Bitrix.</p> <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику записать произвольные файлы в уязвимую систему посредством отправки специально сформированных сетевых пакетов. Данная уязвимость присутствует в модуле «vote» CMS Bitrix.</p> <p>В целях противодействия указанной угрозе рекомендуем отключить или удалить модуль «vote», а также использовать межсетевой экран прикладного уровня.</p> <p>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.</p> |