НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Устранение уязвимости нулевого дня в CMS Bitrix

ALRT-20220303.2v2 | 11 марта 2022 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Уязвимое программное обеспечение	CMS Bitrix
Актуальность угрозы	По настоящее время
Описание	НКЦКИ сообщает о продолжающихся компьютерных атаках злоумышленников, связанных с эксплуатацией критической уязвимости в CMS Bitrix, указанной в бюллетене ALRT-20220303.2. 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. Производителем программного обеспечения оперативно было выпущено исправление указанной уязвимости. Актуальная версия модуля «vote» — 21.0.100. Рекомендуем в кратчайшие сроки провести мероприятия по обновлению данного программного обеспечения. При возникновении проблем с установкой обновления ПО или невозможности установить обновление онлайн, патч с исправлением можно запросить в технической поддержке 1С-Битрикс (https://www.1c-bitrix.ru/support/). 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.