НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Уязвимость в сервисе видеоконференций iMind

ALRT-20230906.1 | 6 сентября 2023 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Описание угрозы	По каналам НКЦКИ поступают сведения об участившихся компьютерных инцидентах, связанных с эксплуатацией уязвимости в сервисе видеоконференций iMind. Эксплуатация указанной уязвимости позволяет злоумышленнику выполнить произвольный код от имени администратора и получить несанкционированный доступ к данным в целевой системе. Уязвимость на данный момент не имеет идентификатора. Признаком эксплуатации уязвимости может быть запуск команды «systemctl restart nginx» от имени системной сервисной учетной записи «monitoring». Во время перезапуска веб-сервера происходит установка вредоносных модулей от имени процесса «nginx». Директории, в которых злоумышленники размещают вредоносные модули: • /usr/bin/atd • /usr/bin/dcrond • /usr/lib/systemd/system/at.service • /usr/lib/systemd/system/dcrond.service Уязвимыми являются версии программного обеспечения iMind до 3.18 включительно.
Рекомендации по нейтрализации угрозы	Обновить программное обеспечение iMind до версии 3.19 или предоставить доступ к сервису из сети Интернет только ограниченному числу доверенных пользователей.