НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Выполнение произвольного кода в VMware vCenter Server

CVE-2021-22005

ALRT-20210924.2 | 24 сентября 2021 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Уязвимое программное обеспечение	VMware vCenter Server: 6.7, 6.7 U3, 6.7 U3a, 6.7 U3b, 6.7 U3c, 6.7 U3d, 6.7 U3e, 6.7 U3f, 6.7 U3g, 6.7 U3h, 6.7 U3i, 6.7 U3k, 6.7 U3l, 6.7 U3m, 6.7 U3n, 6.7.0, 6.7.0d, 7.0, 7.0 U1a, 7.0 U1b, 7.0 U1c, 7.0 U2a, 7.0 U2b
Описание угрозы	Эксплуатация уязвимости в VMware vCenter Server позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных запросов на порт 443/TCP. Уязвимость обусловлена некорректной проверкой файла во время загрузки в сервисе Analytics. Отмечаем, что наличие средств эксплуатации указанной уязвимости не подтверждено, но тем не менее, в настоящее время злоумышленники активно осуществляют поиск хостов, подверженных указанной уязвимости, что в свою очередь в будущем может привести к массовым компьютерным атакам на виртуальные инфраструктуры с целью последующего получения несанкционированного доступа. Для предотвращения компрометации вашей виртуальной инфраструктуры воспользуйтесь рекомендациями, приведенными ниже. Бюллетень НКЦКИ об указанной уязвимости опубликован по следующей ссылке: https://safe-surf.ru/upload/VULN/VULN-20210922.2.pdf
Рекомендации по нейтрализации угрозы	В целях нейтрализации данной угрозы рекомендуем: 1. Обновить VMware vCenter Server до актуальных версий 2. Воспользоваться временными рекомендациями (в случае невозможности обновления VMware vCenter Server) компании VMware доступными по следующему адресу: https://kb.vmware.com/s/article/85717 3. Ограничить доступ к VMware vCenter Server по порту 443/TCP средствами межсетевого экранирования. В случае выявления признаков компрометации ИТС Вашей компании просим сообщить об этом в НКЦКИ.
Ссылки на источники	https://kb.vmware.com/s/article/85717 https://www.tenable.com/blog/cve-2021-22005-critical-file-upload-vulnerability-in-vmware-vcenter-server https://www.cybersecurity-help.cz/vdb/SB2021092117