НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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



# Эксплуатация уязвимостей TrueConf Server APT-группировкой PhantomCore

ALRT-20260817.1 | 17 августа 2026 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

| | |
|---|---|
| Описание угрозы | За последний год нашей организацией зарегистрированы многочисленные целевые компьютерные атаки на российские организации различных отраслей экономики и государственного управления. Атаки осуществляются с использованием как ранее известных, так и новых уязвимостей, обнаруживаемых в устаревших версиях программного обеспечения TrueConf Server.<br><br>Актуальность угрозы подтверждается эксплуатацией злоумышленниками недавно выявленных уязвимостей BDU:2026-11246 и BDU:2026-11247, которые активно используются для компрометации корпоративных сетей.<br><br>BDU:2026-11246 — уязвимость программного обеспечения TrueConf Server, обусловленная отсутствием аутентификации при обращении к критически важным функциям системы. Успешная эксплуатация данной уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе и впоследствии повысить привилегии.<br><br>BDU:2026-11247 — уязвимость программного обеспечения TrueConf Server, обусловленная некорректным управлением генерацией кода. Успешная эксплуатация данной уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе.<br><br>Эксплуатируя указанную связку критических уязвимостей, злоумышленники получают возможность удалённого выполнения произвольного кода с наивысшими системными привилегиями, что позволяет им полностью скомпрометировать сервер, внедрить средства удалённого управления для закрепления в системе, похитить учётные данные из базы данных и модифицировать файлы сервера. В частности, атакующие подменяют легитимный установочный пакет TrueConf Client, в результате чего все участники видеоконференций, подключающиеся к такому серверу, получают предложение установить «обновлённую» версию, которая в действительности содержит вредоносное ПО PhantomCore, обеспечивающее злоумышленникам полный удалённый контроль над рабочими станциями жертв.<br><br>При этом в ряде случаев злоумышленники не ограничиваются использованием только указанных двух уязвимостей, а комбинируют их с ранее выявленными уязвимостями (BDU:2025-10114, BDU:2025-10115, BDU:2025-10116), образуя многоступенчатую цепочку атак.<br><br>Реализация подобных атак создаёт серьёзную угрозу информационной безопасности, так как успешное выполнение всей цепочки даёт нарушителям возможность не только полностью контролировать скомпрометированные серверы и рабочие станции, но и использовать их в качестве плацдарма для дальнейшего распространения вредоносного программного обеспечения. |

| | |
|---|---|
| Рекомендуемые меры по нейтрализации угроз | 1. Выполнить обновление TrueConf Server до актуальной версии в соответствии с рекомендациями разработчика программного обеспечения.<br><br>2. Провести проверку корпоративной инфраструктуры на наличие признаков компрометации с использованием приведённых ниже индикаторов компрометации.<br><br>3. Провести полную внеплановую проверку антивирусным программным обеспечением с актуальными антивирусными базами и программными модулями.<br><br>4. Осуществить проверку всех установочных файлов TrueConf Client, доступных для загрузки с корпоративного сервера, на наличие действительной цифровой подписи разработчика. Вредоносные дистрибутивы, как правило, не имеют корректной цифровой подписи.<br><br>5. В случае подключения сотрудников организации к видеоконференциям на внешних площадках TrueConf их рабочие станции также подвергаются риску, так как на них могли быть установлены инсталляционные пакеты с вредоносным кодом. В кратчайшие сроки провести проверку всех конечных устройств, участвовавших в таких сессиях, с использованием средств антивирусной защиты и при необходимости принять меры по устранению выявленных угроз.<br><br>6. Ознакомиться с публичными материалами АО «Лаборатория Касперского» и ООО «Труконф»:<br>https://ics-cert.kaspersky.ru/publications/reports/2026/08/07/head-mare-exploits-vulnerabilities-in-trueconf-server-to-deliver-phantomcore-malware/<br><br>https://trueconf.ru/blog/update/trueconf-server-security-update-june-2026 |
| Индикаторы компрометации | Контрольные суммы файлов (MD5)<br>4d27b4eb1c5dbb3d8160f29b8119523e – web shell locale.php<br>748c9f8cb10650006162049 35f96207f – вредоносный инсталлятор trueconf_windows_update.exe<br>c5a460e4e68a088f6e51b2c6474642ec – PhantomCore backdoor<br>129462164a7d52e9ea8560b60f0412c5 – doc.txt<br>ec0bf4a2186a88874e9f26f07cfeb532 – usocacheddata.txt<br>b348642146ea34771e5785c5857950f5<br>c915cb6c2aeb863ee8479238e1644217 – doc.txt<br>0e79996d9483d1e44fea32b0a48c2c19 – doc.txt |

2bb75c20e778eb5c416965bd4d4259b1 – trueconf_windows_client_x64_[redacted].exe
b3a6fee3307f1c26841fd5c603e2b013 – usocacheddata.txt
8fcc3e4ccbf1725d9989fb464abf3561 – usocacheddata.txt
489f43be558b2679284ceabed7adc4f3 – модуль транспорта backdoor
0e4541c3153ec5ed01497f19cf4f63d0 – модуль транспорта backdoor
12d4e8f5295f2ef7e0f9bfc0f4830939 – модуль транспорта backdoor
7f267006cac10f341c356b62fe493527 – модуль транспорта backdoor
ee2861d5965e8730708cd1da8a93fa4c – модуль транспорта backdoor
dd1fd2b459b97b7d59375cb8383cd19a – модуль исполнения команд backdoor
4333f52668996c0fa44c14fefba7fecc – файл с токеном backdoor
c3a2abe8756910f42582b04a44ea3514 – backdoor
43f435c3c437bc879a2d7d4634f43494 – backdoor
aee9642b45b099cb7f3053b9b680b425 – rootkit/backdoor

### Пути к файлам

C:\Windows\System32\inetsrv\SysExcSvc.dll
C:\Windows\System32\inetsrv\SysReadSvc.dll
C:\Windows\System32\inetsrv\graphi-refresh.dat
C:\Windows\System32\inetsrv\share\input_*.txt
C:\Windows\System32\inetsrv\share\output_*.txt
%TEMP%\cmd_cmd_*.bat
%LOCALAPPDATA%\TrueConf\Client\api-ms-win-crt-time-l1-1-0-2.dll
/etc/systemd/system/omicluster.service
/etc/systemd/system/schedul2-bin.service
/opt/acronis/bin/schedul2-bin
/omi/bin/omicluster
/usr/lib64/libzvbi-tchain.so.2
/var/tmp/cx2

### IP-адреса и доменные имена

81.177.32[.]12
194.87.239[.]71
194.87.93[.]153
38.244.205[.]244

31.59.102[.]61
penzadogshelter[.]site
trendy-market[.]site
bright-deals[.]site
nova-stream[.]site
rinomobile[.]ink
urbanpixel[.]store
flexish[.]shop
media-hub[.]today
cosmetic-deals[.]store
vks.gossopka[.]forum

### Имена служб Windows
SysExcSvc
SysReadSvc

### Ключи реестра
HKEY_CURRENT_USER\Software\Classes\CLSID\{0340F119-A598-4ed9-B0AC-6F6A12D3E755}\InprocServer32

### Вердикты защитных решений
Backdoor.PHP.WebShell.abi
Backdoor.Win64.PhantomCore.dt
Trojan.Win64.Agent.smgvnc
HEUR:Backdoor.Win64.PhantomCore.gen
HEUR:Backdoor.Linux.Agent.fb
Trojan.Win64.PhantomGraph.gen
Trojan.Win64.Agent.smgvnb
UDS:Backdoor.Win64.PhantomCore.a