НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Множественные уязвимости в TrueConf Server

ALRT-20220606.1 | 6 июня 2022 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

<table>
<tr><td>Актуальность угрозы</td><td colspan="2">Уязвимы все версии TrueConf Server, предшествующие v.4.7.3 и v.5.0.2</td></tr>
<tr><td>Описание угрозы</td><td colspan="2">Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к произвольным файлам посредством проведения атаки типа “Path Traversal”. Уязвимость обусловлена отсутствием в сценарии /handlers/get-img-file.php (путь в файловой системе trueconf_install_path%\httpconf\site\handlers\get-img-file.php) достаточной проверки вводимых пользователем данных. Процессы, запускаемые ПО TrueConf Server на ОС Windows, обладают привилегиями учетной записи локальной системы (NT Authority\SYSTEM), что позволяет злоумышленнику читать любой файл в файловой системе посредством отправки специально сформированного запроса.</td></tr>
<tr><td rowspan="5">MITRE:
CVE не определен</td><td>Вектор атаки</td><td>Сетевой</td></tr>
<tr><td>Взаимодействие с пользователем</td><td>Нет</td></tr>
<tr><td>Последствия эксплуатации уязвимости</td><td>Раскрытие информации</td></tr>
<tr><td>Дата выявления</td><td>31.05.2022</td></tr>
<tr><td>Оценка критичности уязвимости (CVSSv3.0)</td><td>9.3 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:L</td></tr>
<tr><td>Рекомендации по нейтрализации угрозы</td><td colspan="2">Обновить программное обеспечение до v.4.7.3 или v.5.0.2</td></tr>
</table>

<table>
<tr><td>Актуальность угрозы</td><td colspan="2">Уязвимы все версии TrueConf Server, предшествующие v.4.7.3 и v.5.0.2</td></tr>
<tr><td>Описание угрозы</td><td colspan="2">Эксплуатация уязвимости позволяет удаленному злоумышленнику, являющемуся гостем конференции или обладающему действующим api_key, загрузить файл в целевую систему, что может привести к выполнению кода. Уязвимость обусловлена отсутствием в сценарии /client/upsld/v1 достаточной проверки вводимых пользователем данных. Злоумышленник через параметр conf_id, который подвержен атаке Path Traversal, может записать файл с расширением .php в папку, доступную через веб интерфейс.</td></tr>
<tr><td rowspan="5">MITRE:
CVE не определен</td><td>Вектор атаки</td><td>Сетевой</td></tr>
<tr><td>Взаимодействие с пользователем</td><td>Нет</td></tr>
<tr><td>Последствия эксплуатации уязвимости</td><td>Компрометация системы</td></tr>
<tr><td>Дата выявления</td><td>31.05.2022</td></tr>
<tr><td>Оценка критичности уязвимости (CVSSv3.0)</td><td>9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H</td></tr>
<tr><td>Рекомендации по нейтрализации угрозы</td><td colspan="2">Обновить программное обеспечение до v.4.7.3 или v.5.0.2</td></tr>
<tr><td>Выявление признаков эксплуатации уязвимости</td><td colspan="2">1. Обнаружение загрузки исполняемых файлов в лог-файлах:
— $img_url = \Core\WebManager::getInstance()->getUrl() . '/slideshow/' . $conference_call_id . '/' . $new_file_name;
— \header('HTTP/1.1 201 Created');
— \header('Location: ' . $img_url);
— \header('Content-Type: application/json');
— $logger = \TCS\Application\DependencyContainer::getInstance()->get('App\\Log\\LoggerInterface');
— $logger->trace(['URL' => $img_url]);
2. Поиск в логах веб-сервера:
— cat weblog\site.log | grep -iF "\\slideshow\\" | grep -iF ".php"
— cat web_logs\log_* | grep -iF "readfile(" | grep -iF "get-img-file.php"</td></tr>
<tr><td>Ссылки на источники</td><td colspan="2">https://www.kaspersky.ru/about/press-releases/2022_laboratoriya-kasperskogo-obnaruzhila-kriticheskie-uyazvimosti-v-trueconf-server
https://trueconf.ru/blog/news/tcs-security-update-5-0-2.html</td></tr>
</table>