**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

**ОТЧЁТ**

**GitLab Pre-Auth RCE (CVE-2021-22205)***(тема отчета)*

Направление/специальность подготовки

10.03.01 «Информационная безопасность»

*(код и наименование направления/специальности)*

Выполнили:

Ли Ю.А., ИКБ-05  
Ким В.Ю., ИКБ-05  
Гречухин Д.Н., ИКБ-05

*(Ф.И.О., № группы)*

Преподаватель:

к.т.н. Виткова Л.А., доцент каф. ЗСС

*(уч. степень, уч. звание, Ф.И.О.)*

Оглавление

[Теоретические сведения об уязвимости 3](#_Toc145086449)

[Rapid7 анализ. Путь атаки и эксплойт 5](#_Toc145086450)

[Руководство по воздействию и смягчению последствий 8](#_Toc145086451)

Теоретические сведения об уязвимости

Описание:  
CVE-2021-22205 — критическая уязвимость удаленного выполнения кода в веб-интерфейсе сервиса.

Главной причиной возникновения данной уязвимости была некорректная обработка загружаемых файлов с изображениями парсером на базе библиотеки ExifTool. (позже этой уязвимости был присвоен номер 2021-22204).

Принцип работы:

При загрузке изображений в GitLab любой формат изображений передается в утилиту, позволяющую стирать все метаданные, которая использует библиотеку ExifTool. Один из поддерживаемых форматов - DjVu. Удаленный злоумышленник мог выполнить произвольные команды от имени пользователя git из-за неправильной обработки ExifTool файлов DjVu. По сути, эта проблема дает атакующему полный доступ к репозиторию, включая удаление, изменение и кражу исходного кода.

Затронутые продукты:

Согласно бюллетеню безопасности GitLab от апреля 2021 года, CVE-2021-22205 затрагивает все версии GitLab Enterprise Edition (EE) и GitLab Community Edition (CE), начиная с 11.9. Уязвимость исправлена в следующих версиях:

13.10.3

13.9.6

13.8.8

Оценка по шкале CVSS v3:

Уязвимость имеет идентификатор CVE-2021-22205 и максимально возможную оценку по шкале CVSS v3 — 10 баллов ровно. Изначально считалось, что уязвимость требует аутентификации, и ей была присвоена оценка 9,9 балла по шкале CVSS, но 21 сентября 2021 года это решение пересмотрели, когда стало ясно, что аутентификация не требуется.

Первая подтверждённая атака хакерами с использованием данной уязвимости была замечена в июне 2021 года. Тогда ошибка применялась для создания новых пользователей и предоставления им прав администратора. Существует несколько опубликованных общедоступных эксплойтов для этой уязвимости.

Всем пользователям рекомендуется обновить свою версию GitLab до последней (она должна быть выше, чем 13.10.3).

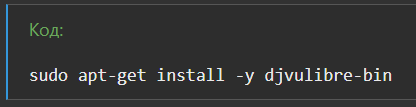
GitLab не должен быть открытым для интернета сервисом. Если вам нужно получить доступ к GitLab из интернета, рассмотрите возможность размещения его за VPN или 2FA.

Rapid7 анализ. Путь атаки и эксплойт

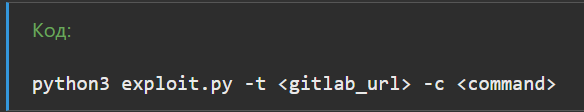
Процесс установки самого эксплоита будет таковым:



Прежде нужно удостовериться имеются ли библиотеки djvumake & djvulibre, установить можно следующей командой:



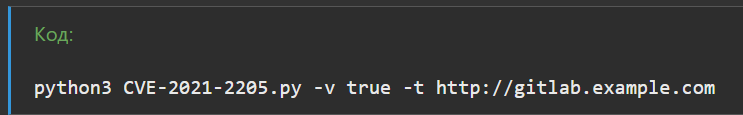
После ввода следующей команды, выполняем её на удаленной машине:



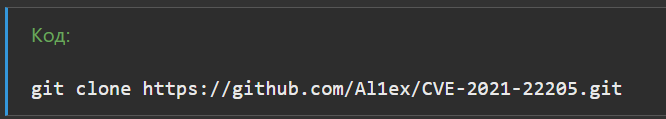


Существует более продуманный эксплойт по этой уязвимости, рассмотрим его более детально:

Некий умелый пользователь GitHub разработал на базе предыдущего скрипт, который умеет проверять уязвим ли хост на предмет эксплуатации:



Установить его можно так:



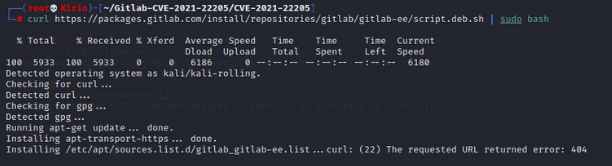
Таким образом, можно увидеть подвержено ли устройство атаке. Пробуем полнить какую-нибудь команду, например, скачивание простого текстового файла из интернета:

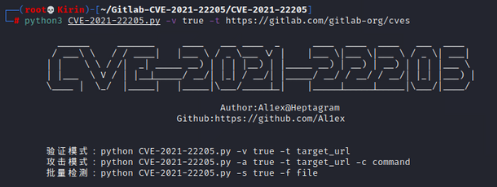


Можем вывести какое-то сообщение в терминал и открыть сам codeby.txt:



Также попытки выгрузить любую полезную нагрузку и запустить слушатель через curl – венчаются успехом.





curl — это набор библиотек, в которых реализуются базовые возможности работы с URL страницами и передачи файлов. Библиотека поддерживает работу с протоколами: FTP, FTPS, HTTP, HTTPS, TFTP, SCP, SFTP, Telnet, DICT, LDAP, а также POP3, IMAP и SMTP. Она отлично подходит для имитации действий пользователя на страницах и других операций с URL адресами.

Руководство по воздействию и смягчению последствий

Чтобы определить, затронуты ли вы этой уязвимостью, изучите журнал gitlab-workhorse. В Ubuntu он расположен в /var/log/syslog/gitlab/gitlab-workhorse/.

Обратите внимание, что исправленная версия GitLab также будет иметь журналы gitlab-workhorse о попытках эксплуатации. Они будут выглядеть примерно так:

{"correlation\_id":"01FKC13E1EE91VWC0B9M16YF58","filename":"test.jpeg","imageType":1,"level":"info","msg":"неверный тип контента, exiftool не запущен","time" :"2021-10-31T13:36:52-07:00"}

Вы также можете найти что-то вроде следующего, /var/log/gitlab/nginx/gitlab\_access.log, но поскольку запросы могут отправляться POST к произвольным конечным точкам, это может быть не очень полезно.

Наконец, можно определить, уязвим ли удаленный экземпляр GitLab, на основе его  
ответа на запрос POST. Например:

albinolobster@ubuntu:~$ echo lollol > test.jpeg

albinolobster@ubuntu:~$ curl -v -F 'file=\*\*[@test](/contributors/test)\*\*.jpeg' http://10.0.0.7/$(openssl rand -hex 8)

Неисправленная версия ответит ответом HTTP 422 и текстом «\*Запрошенное вами изменение было отклонено». Исправленная версия GitLab ответит ответом HTTP 404 и текстом «\*Страница не найдена…\* ».

Как было сказано в начале: пользователям GitLab следует как можно скорее обновиться до последней версии GitLab. В идеале GitLab не должен быть интернет-сервисом. Если вам нужен доступ к GitLab из Интернета, рассмотрите возможность размещения его через VPN.

Список используемых источников

1. Интернет-ресурс: https://attackerkb.com/topics/D41jRUXCiJ/cve-2021-22205/rapid7-analysis
2. Интернет-ресурс: https://codeby.net/threads/sve-2021-22205-udalennoe-vypolnenie-koda-na-serverax-gitlab.78952/
3. Интернет-ресурс: https://nvd.nist.gov/vuln/detail/CVE-2021-22205
4. Интернет-ресурс: https://www.anti-malware.ru/news/2021-11-02-114534/37367