접수자 정보			
접 수 번 호	20230630		
성 명	루키즈	접 수 일 자	2023. 06. 29
분석자 정보			
성 명	송승현, 신동석, 김규식, 최영흠, 전유진, 우상준, 이혜담, 김정윤	분 석 일 자	2023. 06. 29~2023. 06. 30
침해사고 개요			
사 고 개 요	원격 코드 실행 취약점으로 인한 공격		
사 고 원 인	최신 버전의 애플리케이션을 사용하지 않아 GitStack 2.3.10 버전의 원격 코드 실행 취약점에 노출됨		

분 석 결 과
(피 해 현 황)

1. Rootkit 점검 결과 피해자 시스템 운영체제 확인

vol.exe -f IR01.raw imageinfo

```
D:₩vol>vol.exe -f IR01.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:₩vol₩IR01.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82b7fc30L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82b80c00L
                KPCR for CPU 1 : 0x807cb000L
                KPCR for CPU 2 : 0x8b515000L
                KPCR for CPU 3 : 0x8b550000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-07-06 14:03:57 UTC+0000
     Image local date and time : 2019-07-06 07:03:57 -0700
```

2. 프로세스 목록 및 스케줄링 된 프로세스 정보

vol.exe -f IR01.raw --profile=Win7SP1x86 pslist/psscan

pslist.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
0x889bf8d0 conhost.exe        2124   428    2     50     1      0 2019-07-06 13:40:36 UTC+0000
0x86b01d40 cmd.exe            1156   1920   1     21     1      0 2019-07-06 13:45:43 UTC+0000
0x86418498 conhost.exe        2696   428    2     49     1      0 2019-07-06 13:45:43 UTC+0000
0x864e39c8 httpd.exe          3044   3692   70    329    1      0 2019-07-06 13:47:11 UTC+0000
0x88a02d40 mmc.exe            2600   1920   30    621    1      0 2019-07-06 13:50:39 UTC+0000
0x854a7030 cmd.exe            1260   1920   1     21     1      0 2019-07-06 13:52:49 UTC+0000
0x858f5d40 conhost.exe        1020   428    2     49     1      0 2019-07-06 13:52:49 UTC+0000
0x86995910 Sysmon.exe         3568   476    10    190    0      0 2019-07-06 13:53:52 UTC+0000
0x869ac030 unsecapp.exe       416    636    4     67     0      0 2019-07-06 13:53:52 UTC+0000
0x86c303c8 cmd.exe            2956   3044   0 --------   1      0 2019-07-06 13:56:57 UTC+0000   2019-07-06 13:56:57 UTC+0000
0x86505660 openssl.exe        2712   2956   0 --------   1      0 2019-07-06 13:56:57 UTC+0000   2019-07-06 13:56:57 UTC+0000
0x88768030 powershell.exe     2944   1740   0 --------   1      0 2019-07-06 13:56:57 UTC+0000   2019-07-06 13:56:57 UTC+0000
0x85971a60 powershell.exe     1240   2944   8     294    1      0 2019-07-06 13:56:57 UTC+0000
0x86c69030 conhost.exe        3684   428    1     32     1      0 2019-07-06 13:56:57 UTC+0000
0x870f3570 cmd.exe            2236   1240   0 --------   1      0 2019-07-06 13:57:50 UTC+0000   2019-07-06 13:58:32 UTC+0000
```

- cmd.exe
- openssl.exe
- powershell.exe

3. 예약 중인 프로그램 확인

vol.exe -f IR01.raw --profile=Win7SP1x86 netscan | findstr LISTENING

```
D:₩vol>vol.exe -f IR01.raw --profile=Win7SP1x86 netscan | findstr LISTENING
Volatility Foundation Volatility Framework 2.6
0x7c4f14a0         TCPv4    0.0.0.0:80                     0.0.0.0:0              LISTENING        3692    httpd.exe
0x7c4f14a0         TCPv6    :::80                          :::0                   LISTENING        3692    httpd.exe
0x7c909b00         TCPv4    0.0.0.0:80                     0.0.0.0:0              LISTENING        3692    httpd.exe
0x7e3179e0         TCPv4    0.0.0.0:5357                   0.0.0.0:0              LISTENING        4       System
0x7e3179e0         TCPv6    :::5357                        :::0                   LISTENING        4       System
0x7e42e8d8         TCPv4    0.0.0.0:445                    0.0.0.0:0              LISTENING        4       System
0x7e42e8d8         TCPv6    :::445                         :::0                   LISTENING        4       System
0x7e442970         TCPv4    0.0.0.0:49155                  0.0.0.0:0              LISTENING        476     services.exe
0x7e442970         TCPv6    :::49155                       :::0                   LISTENING        476     services.exe
0x7e46e4b0         TCPv4    0.0.0.0:49156                  0.0.0.0:0              LISTENING        492     lsass.exe
0x7e46e4b0         TCPv6    :::49156                       :::0                   LISTENING        492     lsass.exe
0x7e46e558         TCPv4    0.0.0.0:49156                  0.0.0.0:0              LISTENING        492     lsass.exe
0x7e52a898         TCPv4    0.0.0.0:3389                   0.0.0.0:0              LISTENING        1204    svchost.exe
0x7e52ca28         TCPv4    0.0.0.0:3389                   0.0.0.0:0              LISTENING        1204    svchost.exe
0x7e52ca28         TCPv6    :::3389                        :::0                   LISTENING        1204    svchost.exe
0x7e656428         TCPv4    192.168.130.131:139            0.0.0.0:0              LISTENING        4       System
0x7e7a2008         TCPv4    0.0.0.0:49155                  0.0.0.0:0              LISTENING        476     services.exe
0x7e913108         TCPv4    0.0.0.0:135                    0.0.0.0:0              LISTENING        760     svchost.exe
0x7e915778         TCPv4    0.0.0.0:135                    0.0.0.0:0              LISTENING        760     svchost.exe
0x7e915778         TCPv6    :::135                         :::0                   LISTENING        760     svchost.exe
```

침해사고 시스템 정보	
호스트/도메인명	IEUser
호 스 트 용 도	웹 기반의 소스 코드 관리 서버
IP 주 소	192.168.130.131
하 드 웨 어 및 OS 정보	CPU 수: 4 OS 정보: IE11Win7

대응방안 및 미 조치사항 권고	
수행항목	대응방안 및 권고사항
악성코드 제거	c:\GitStack\gitphp에 위치해 있는 exploit.php 웹쉘을 삭제
계정 확인	공격자에 의해 GitStack에 생성된 rce 계정을 삭제
앱 업데이트	최신버전인 GitStack 2.3.14으로 업데이트
비밀번호 강화	문자, 숫자, 대문자/소문자, 기호를 조합하여 일반적인 단어나 이름과 전혀 상관없는 예측할 수 없는 문자열로 안전한 비밀번호 생성

기타 특이사항

침해 과정

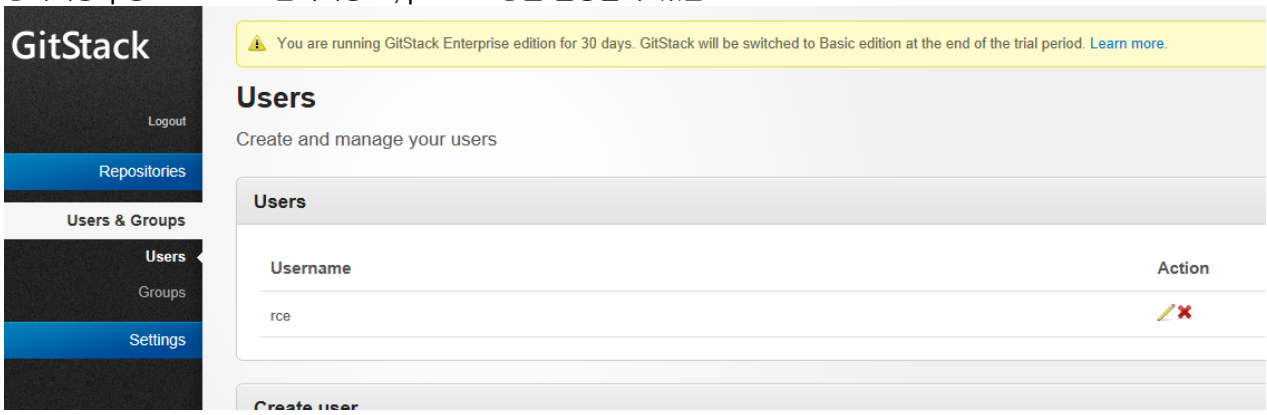
환경을 구축하고 공격코드를 이용하여 시나리오 모의해킹 수행

```
└─# sudo python2 /home/kali/Downloads/43777.py
[+] Get user list
[+] Create user
[+] Web repository already enabled
[+] Get repositories list
[+] Create repository
[+] Add user to repository
[+] Disable access for anyone
[+] Create backdoor in PHP
Your GitStack credentials were not entered correcly. Please ask your GitStack administrator to give you a username/passwor
d and give you access to this repository. <br />Note : You have to enter the credentials of a user which has at least read
 access to your repository. Your GitStack administration panel username/password will not work.
[+] Execute command
"nt authority\system
"
```

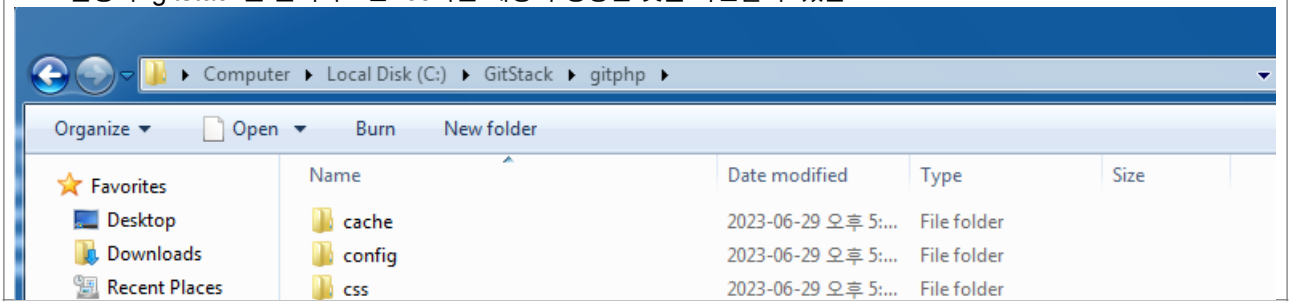
exploit-db에서 git stack2.3.10 코드를 다운받고 공격할 ip를 수정한 다음에 실행

```
#
import requests
from requests.auth import HTTPBasicAuth
import os
import sys

ip = '192.168.10.130'

# What command you want to execute
command = "whoami"

repository = 'rce'
username = 'rce'
password = 'rce'
csrf_token = 'token'
```

공격대상 ip랑 command입력이랑 id, passwd등을 설정할 수 있음



코드 실행 후 gitstack를 들어가보면 rce라는 계정이 생성된 것을 확인할 수 있음



시스템 점검 방안
내부 네트워크를 통한 이차 전이공격가능성에 대비하여 각 시스템에서 아래의 사항에 대하여 점검이 필요함 1. 패스워드 변경 유무 2. 시스템 CPU 상태 확인 3. 비 인가된 사용자 접근 4. 시스템 로그 5. 시스템 세션 확인