



외부 네트워크 침투 테스트 보고서

준비
RVAPT 호스팅

날짜
2020년 4월 22일

의해서 준비되었다
레드포스X

버전
1.0

- 라이언 세르반테스
- 호르헤 플로레스
- 막스 푸스코
- 락쉬마난 머티

목차

| | |
|---|----|
| 목차 | 2 |
| 요약 | 4 |
| 참여 개요 | 5 |
| 측정항목 | 6 |
| CVSS(Common Vulnerability Scoring System) 위험, | 6 |
| 영향, 가능성 | 7 |
| 비즈니스 영향 규모 | 7 |
| 위험 매트릭스 | 8 |
| 평가 요약 | 9 |
| 환경 | 9 |
| 측정항목 | 10 |
| 취약점 분석 손상률 | 10 |
| | 11 |
| 중요한 발견들 | 12 |
| 공격 내러티브 | 13 |
| 정찰 및 열거 | 13 |
| 착취 및 착취 후 | 13 |
| 외부(클라이언트) 네트워크 | 13 |
| 내부(기업) 네트워크 | 13 |
| 결과 | 15 |
| 일반 텍스트 자격 증명 | 15 |
| 인증되지 않은 MySQL | 18 |
| 침해 지표 관리자 허용 외부 액세스 | 20 |
| SMBV1 활성화됨 | 22 |
| | 23 |
| 노출된 MySQL | 25 |
| Miniserv 원격 코드 실행 루트 실행 애플리 | 27 |
| 케이션 | 29 |
| OSCommerce 원격 코드 실행 로컬 관리자 자격 | 31 |
| 증명 재사용 | 33 |
| C:\Windows 폴더 SMB FTP 익명 로그인에 | 34 |
| 서 호스팅됨 | 35 |
| 폐기된 FTP 서버 | 37 |

| | |
|--------------------|----|
| 안전하지 않은 HTTP | 38 |
| Bricktube 원격 코드 실행 | 39 |

| |
|----|
| 38 |
| 39 |

요약

Red Force X는 2020년 4월 6일부터 2020년 4월 17일까지 RVAPT Hosting의 인프라에 대한 외부 및 내부 보안(또는 "침투 테스트" 또는 "침투 테스트") 감사를 수행하기로 계약했습니다. 이 침투 테스트의 목적은 사이버 공격을 평가하는 것이었습니다. -외부 스레드 액터의 공격을 방어하기 위한 RVAPT 호스팅 준비 상태. Red Force는 이 보고서를 통해 RVAPT 호스팅의 보안 취약점에 대한 자세한 개요를 제공하고 인프라 보안을 강화하기 위한 수정 단계를 권장합니다.

침투 테스트를 마친 레드포스X는 **다수의 주요 취약점 식별** RVAPT Hosting의 네트워크에 가장 큰 피해를 줄 수 있는 이러한 취약점은 평가자에게 **RVAPT Hosting이 소유한 모든 시스템에 대한 중요한 액세스**. RVAPT Hosting의 일상적인 작업 맥락에서 이러한 취약점은 다음과 같은 결과를 초래합니다.

- 회사 네트워크의 완전한 인수
- 일상 업무의 중단 또는 중단
- 고객 데이터 손실

Red Force X는 RVAPT Hosting과 클라이언트의 최대 이익을 보호하기 위해 앞서 언급한 상황을 방지하기 위해 이 문서에 설명된 수정 조치를 적시에 구현할 것을 권장합니다. 일반적으로 Red Force X의 권장 사항은 **수정, 적당한 노력, 비용 및 가동 중지 시간이 필요합니다**. 안전한 외부 인프라를 보장합니다. 필요한 주요 비용과 노력은 복구할 수 없는 보안 취약성으로 인해 RVAPT Hosting 운영에 중요한 특정 소프트웨어를 교체하는 것입니다. 그렇지 않으면 발견된 대부분의 다른 취약점은 많은 리소스가 필요하지 않으며 소프트웨어 업데이트 및 정책 변경을 통해 쉽게 패치할 수 있습니다.

Red Force X는 RVAPT Hosting이 필요한 모든 수정 사항을 구현할 수 있는 능력을 가지고 있다고 확신합니다. 또한 가능한 경우 Red Force X 보안 컨설턴트도 지원을 제공할 수 있습니다.

참여 개요

Red Force X에서 수행하는 이 평가의 목적은 민감한 정보 기술(IT) 시스템 및 데이터의 무결성을 보호하기 위해 RVAPT 호스팅에 적용되는 보안 조치의 적절성과 효율성을 테스트하는 것입니다. 이 평가는 RVAPT Hosting IT 시스템의 위험과 취약성을 측정 및 식별하고 실제 공격이 발생할 경우 해당 시스템의 구성, 정책 및 절차의 효율성과 준비성을 평가하는 데 사용됩니다.

이 작업 동안 Red Force X의 목표는 RVAPT Hosting의 외부 기반 인프라에서 보안 취약성을 찾아 악용하는 것이었습니다. 여기에는 웹 서버, 파일 전송 서버 및 원격 로그인 서버와 같은 서비스가 포함됩니다. 이것은 초기 계약에서 Red Force X에 제공되었으며 Red Force X와 RVAPT Hosting이 합의한 "RFP"(제안 응답)에서 확인되었습니다. 테스트 범위는 다음과 같았습니다.

| IP 공간 | 호스트 |
|--------------------------|--|
| 192.168.110.0/24 (외부) | 192.168.110.10 192.168.110.12 192.168.110.14 192.168.110.20 192.168.110.60 |
| 192.168.120.0/24 (내부) | 192.168.120.1 192.168.120.2 192.168.120.18 192.168.120.20 192.168.120.21 |

측정항목

CVSS(Common Vulnerability Scoring System)

비즈니스 인프라에서 발견된 취약성이 얼마나 피해를 주는지 평가하기 위해 두 가지 측정 기준을 사용합니다. Common Vulnerability Scoring System은 시스템의 기밀성, 무결성 및 가용성에 대한 복잡성, 접근성 및 영향으로 취약점을 측정하는 보편적으로 허용되는 개방형 표준입니다. 이것은 대응자가 어떤 취약점을 어떤 순서로 수정해야 하는지 우선 순위를 지정하는 데 사용됩니다. 취약성은 응답 팀에 정보 가치를 제공하는 0.0부터 즉시 처리해야 하는 가장 심각한 취약성을 나타내는 10.0까지 등급으로 분류됩니다.

| 점수 | 설명 |
|---|---|
|  | 중대한 위험 취약점은 이 서비스에 치명적인 영향을 미칩니다. 이 수준의 취약성은 일반적으로 영향을 받는 호스트와 호스트가 상주할 수 있는 네트워크를 완전히 손상시킵니다. 대부분의 경우 악용에는 지식이 거의 또는 전혀 필요하지 않으며 쉽게 구현할 수 있습니다. |
|  | 위험 취약점은 잠재적인 민감한 정보에 액세스할 수 있으며 서비스 거부(DOS) 상태를 유발할 수 있습니다. 심각한 위험 문제보다 악용하기 어려운 문제이므로 심각도가 낮습니다. |
|  | 중간 위험 취약점은 대부분 조직의 비즈니스에 눈에 띄는 영향을 미치기 위해 추가적인 결정과 기술적 능력을 필요로 합니다. 경우에 따라 이러한 문제는 자금 지원 프로젝트와 같은 사람만 사용할 수 있는 높은 수준의 리소스가 필요합니다. |
|  | 낮은 위험 취약점은 조직의 비즈니스에 거의 영향을 미치지 않습니다. 이러한 취약점을 악용하려면 로컬 권한이 있는 액세스가 필요하거나 다른 결과와 함께 사용되어야 합니다. |

위험, 영향, 가능성

우리가 사용하는 두 번째 메트릭은 특정 취약성이 회사에 미치는 비즈니스 영향을 측정하는 내부 척도입니다. 위험, 영향 및 가능성의 세 가지 관련 주제에 대한 취약성을 평가합니다. 영향 취약점이 비즈니스에 미치는 잠재적인 영향을 평가하려는 시도로, 취약점이 비즈니스의 일상적인 운영에 미치는 영향이 클수록 더 심각한 것으로 평가됩니다. 가능성은 위험 행위자가 실행할 취약성의 추정치입니다. 취약성을 악용하는 것이 덜 복잡할수록 심각도가 높아집니다. 위험은 영향(Impact)과 가능성(Likelihood)의 조합으로, 취약점이 악용될 경우의 위험을 측정합니다. 위험이 높을수록 회사에 더 많은 피해를 줄 수 있습니다.

비즈니스 영향 규모

| | 낮은 | 중간 | 높은 |
|-----------|---------------------------------------|--|---------------------------------------|
| 영향 | 악용될 경우, 일상적인 비즈니스 운영은 매우 존재의 작은 변화 방해 | 악용되면 매일 사업 운영 영향을 받을 수 있습니다 | 악용되면 매일 사업 운영 영향을 받을 것이다 |
| 있을 수 있는 일 | 낮은 이 가능성 취약성은 에 의해 악용 경험하고 미숙한 적 | 숙련된 적에게 악용될 가능성이 높습니다. 그리고 더 낮은 확률 미숙한 적 | 이 취약점은 악용하기 쉬운 아마도 에 의해 악용 경험하고 미숙한 적 |
| 위험 | 관련된 위험이 거의 또는 전혀 없습니다. 이 취약점 착취당하고 있다 | 기업 자산에 대한 위험이 높습니다. 이 경우 위험 취약점은 착취 | 기업 자산에 대한 위험이 높습니다. 이 경우 위험 취약점은 착취 |

위험 매트릭스

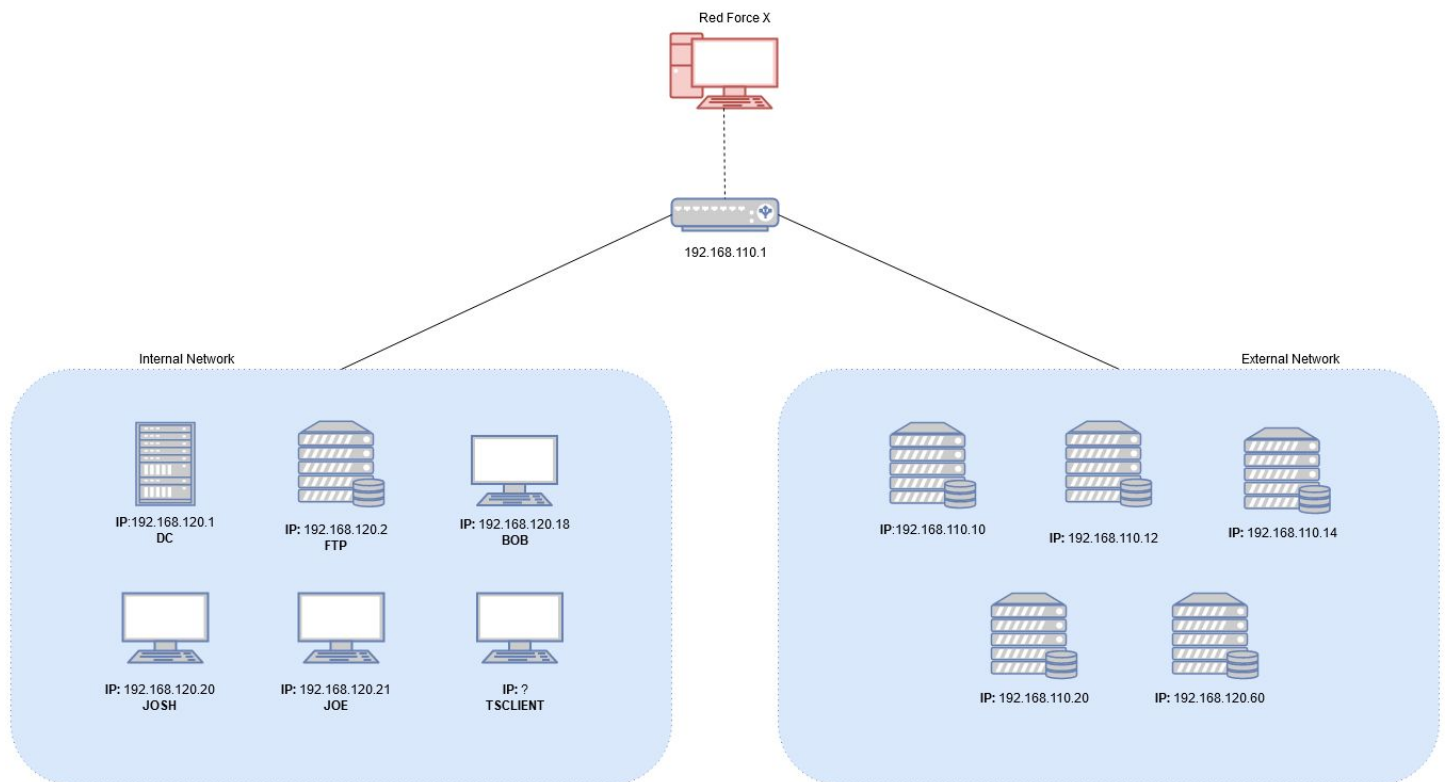
아래 표시된 위험 매트릭스는 특정 취약성이 생성할 다양한 가능성과 영향의 조합을 시각화한 것입니다. 인프라 개선의 우선순위를 정할 때 높음 및 중간 높음은 해당 악용을 수행하는 데 필요한 지식과 복잡성이 낮기 때문에 가능한 한 빨리 수정해야 하는 최우선 순위로 고려해야 합니다. 위험 점수가 감소함에 따라 일반적으로 특정 취약점에 대한 악용을 수행하기 위한 복잡성과 지식이 공격자를 단념시킬 만큼 커집니다. 그러나 강력한 인프라를 보장하려면 적절한 보안 통제가 마련되어야 합니다.

| 위험 매트릭스 | | 영향 | | | | |
|-----------------------------------|-----------------|----------|-------|----------|----------|----------|
| | | 무시할 수 있는 | 미성년자 | 보통의 | 중요한 | 비판적인 |
| 엘 나 케이 엘 나 시간 영향 디 | 가능성이 매우 높다 | 낮은 중간 | 중간 | 중간 높은 | 높은 | 높은 |
| | 할 것 같은 | 낮은 | 낮음 중간 | 중간 | 중간 높은 | 높은 |
| | 가능한 | 낮은 | 낮음 중간 | 중간 | 중간 높은 | 중간 높은 |
| | 할 것 같지 않은 | 낮은 | 낮음 중간 | 낮은 중간 | 중간 | 중간 높은 |
| | 매우 할 것 같지 않은 | 낮은 | 낮은 | 낮은 중간 | 중간 | 중간 |

평가 요약

환경

계약을 맺을 때 Red Force X에는 외부 서브넷용 IP 공간 외에 RVAPT Hosting의 네트워크 토폴로지에 대한 정보가 표시되지 않았습니다. 이 백서에 설명된 주제를 명확히 하기 위해 Red Force X는 이 보고서의 기술적 발견의 기반이 될 토폴로지를 생성했습니다. 이 토폴로지는 서비스를 통해 얻은 정보를 통해 생성되었습니다. 아래 다이어그램은 범위 내에 있었고 계약에서 발견된 호스트만 보여줍니다. 따라서 192.168.110.104 및 192.168.110.254는 나열되지 않습니다.

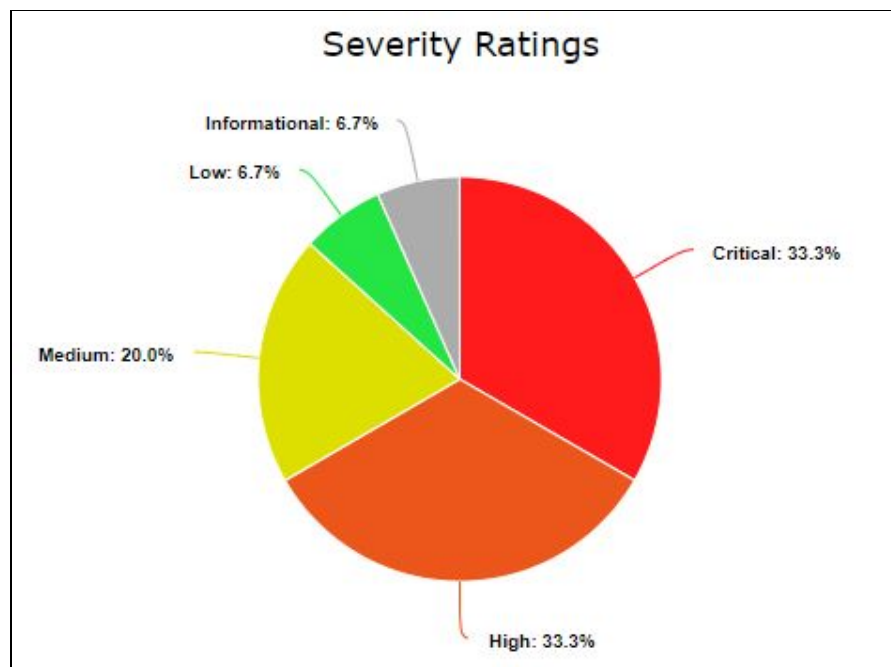


측정항목

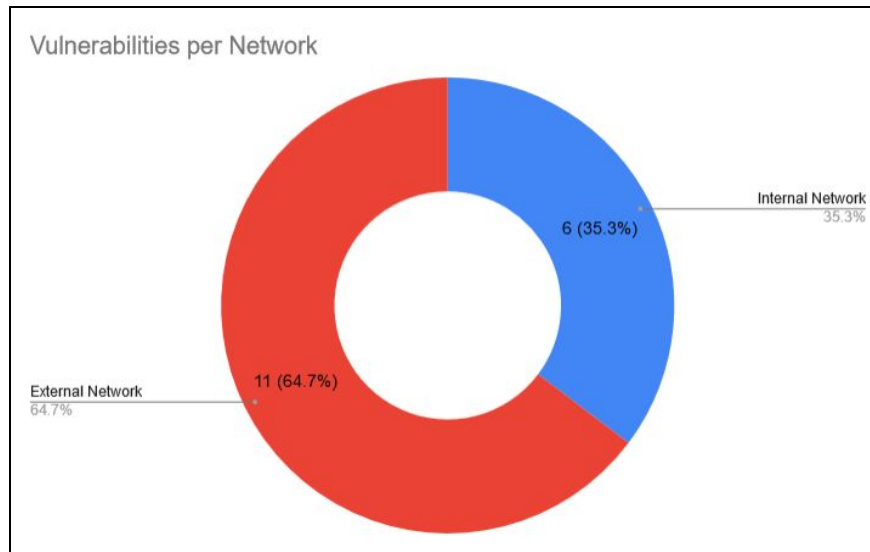
이 섹션에서는 전체 참여에서 가져온 메트릭을 간략하게 설명하고

취약점 분석

Red Force X는 RVAPT Hosting의 기업 및 클라이언트 컴퓨터에서 사용되는 모든 컴퓨터에서 15개의 취약점을 식별할 수 있었습니다. 발견된 대부분의 취약점은 다음 중 하나로 평가되었습니다. **중요** 또는 **높음**, 또는 전체의 67%.

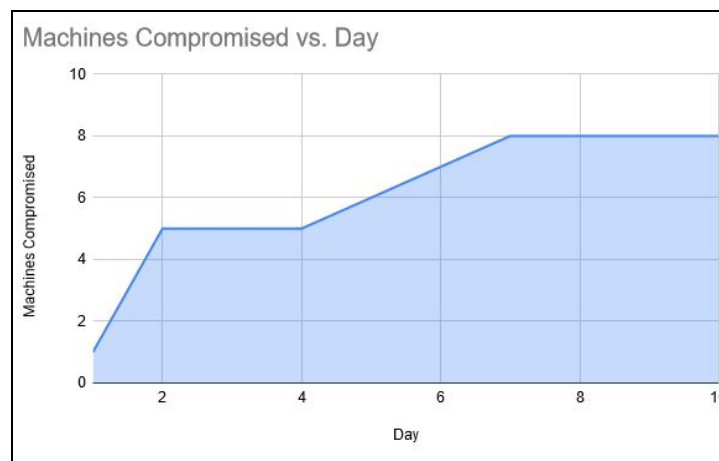


각각의 개별 네트워크와 관련하여 특정 취약점이 두 네트워크 모두에 나타났고 나머지는 각 네트워크에 고유했습니다. 아래 차트는 각 네트워크에서 발견된 취약점 수의 분석을 보여줍니다.



타협률

계약 기간 동안 Red Force X는 범위 내 기계 10대를 식별할 수 있었습니다. 이 중 10일 평가 기간 내에 컴퓨터의 8% 또는 80%에 빠르게 액세스할 수 있었습니다. Red Force X는 먼저 나머지 외부 시스템에 대한 액세스를 허용하는 외부 네트워크(192.168.110.60)의 단일 시스템을 손상시킬 수 있었으며, RVAPT Hosting의 전체 고객 네트워크는 참여 둘째 날까지 손상될 수 있었습니다. 거기에서 Red Force X는 회사 네트워크에 대한 자격 증명을 찾을 때까지 고객 네트워크에서 취약점을 찾는 데 3일을 보냈습니다. 회사 네트워크에 액세스한 후 직원 3대의 컴퓨터에 액세스할 수 있었지만 전체 회사 네트워크를 손상시킬 수는 없었습니다.



중요한 발견들

RVAPT 호스팅에 대한 Red Force X의 평가 중에 함께 악용될 경우 RVAPT 호스팅 웹 사이트의 최소 80%가 공격자에 의해 손상되는 3가지 취약점을 식별할 수 있었습니다. 따라서 이 섹션에 나열된 다음 취약성은 인프라 내에서 수정해야 하는 주요 취약성과 악의적인 결과를 간략하게 설명합니다.

안전하지 않게 관리되는 자격 증명 -이 취약점은 인프라 내에서 인증 시스템을 적절하게 생성, 저장 및 관리하는 기능을 나타냅니다. Red Force X가 참여하는 동안 우리는 비밀번호가 일반 텍스트로 저장되는 여러 인스턴스와 취약한 비밀번호를 발견했습니다. 공격자가 암호를 해독하기 어렵게 하려면 직원이 따라야 할 강력한 암호 정책을 만드는 것이 중요합니다. 최소 길이, 기호, 대문자 및 소문자로 구성되어야 합니다. 자격 증명 저장과 관련하여 암호는 복잡할수록 기억하기 어려울 수 있지만 회사에서 이러한 암호를 쉽게 저장하는 데 사용할 수 있는 소프트웨어 옵션이 있습니다.

오래된 소프트웨어 -이 취약점은 공격자가 해당 소프트웨어 및 시스템을 쉽게 악용할 수 있는 알려진 취약점이 있는 오래된 응용 프로그램을 계속 사용하는 것을 말합니다. 우리가 참여하는 동안 Red Force X는 기업 파일 공유에 사용되는 오래된 SMB뿐만 아니라 고객 웹 사이트를 통해 외부 네트워크에서 여러 응용 프로그램을 사용할 수 있었습니다.

맬웨어 결과 -평가 중에 우리는 Red Force X가 암호 화폐 채굴기로 추정하는 "legionminer"라는 잠재적으로 원치 않는 소프트웨어의 존재를 식별할 수 있었습니다.

공격 내러티브

이 평가를 위해 Red Force X에는 조직 도메인(rvapthosting.com)에 대한 최소한의 정보가 제공되었습니다. 이 평가의 목적은 외부 악의적인 공격자의 행동과 결과를 가능한 한 가깝게 반영하는 것이었습니다. 우리는 외부 네트워크(192.168.110.0/24)와 오프 리미트 머신의 IP 공간만 받았습니다. 거기에서 우리는 외부 네트워크를 평가하고 내부 회사 네트워크를 침투 테스트하는 임무를 받았습니다.

정찰 및 열거

참여 1일차에 Red Force X는 192.168.110.0/24 네트워크의 모든 호스트에 대한 NMAP 스캔을 수행하여 이 평가를 시작했으며, 5개의 대상이 가능한 IP 주소와 금지된 192.168.110.104 및 범위 DNS 서버의 192.168.110.254. 그 후 각 호스트의 특정 서비스에 대한 서비스 및 버전 열거가 수행되어 SSH, FTP 및 VNC와 같은 서비스뿐만 아니라 클라이언트를 위한 많은 웹 서버가 드러났습니다.

착취 및 착취 후

외부(클라이언트) 네트워크

참여 1일차에 Red Force X는 192.168.110.60에 있는 단일 시스템을 식별하고 악용하여 시스템에 대한 루트 액세스를 허용할 수 있었습니다. 이 호스트에서 Red Force X는 관리자가 사용하는 SSH 개인 키로 인해 외부 네트워크의 나머지 호스트를 손상시킬 수 있었습니다.**rvaptsupport** 사용자. 또한 이 호스트는 Red Force X가 회사 네트워크에 액세스할 수 있도록 허용했습니다. **일반 텍스트 관리자 자격 증명 노출** 192.168.120.0/24의 IP 공간 내에 있는 해당 관리자의 컴퓨터도 마찬가지입니다. 나머지 외부 네트워크의 경우 Red Force X는 이 보고서의 "발견 사항" 섹션에 나열된 여러 취약점을 식별할 수 있었습니다.

내부(기업) 네트워크

일주일 간의 외부 네트워크 테스트 후 Red Force X는 내부 네트워크 평가를 시작했습니다. 이 네트워크에서 우리는 5대의 컴퓨터를 찾았는데 그 중 3대는 직원 컴퓨터이고 2대는 도메인 컨트롤러 및 FTP 서버와 같은 회사 컴퓨터였습니다. 내부 네트워크를 테스트하기 위해 시스템에 대한 액세스 권한을 얻기 위해 이전에 찾은 시스템 관리자의 자격 증명을 활용했습니다. 거기에서 Red Force X는 "해제된" FTP 서버에 액세스할 수 있었습니다.**CEO 자격 증명**. 그런 다음 이 두 세트의 자격 증명을 사용하여 LSA 비밀을 추출했습니다.

Red Force X가**자격 증명 재사용을 통해 컴퓨터 3대의 로컬 관리자.**

결과

| # 1 - PLAINTEXT 자격 증명 | | CVSS |
|-----------------------|----------------------------------|--------------|
| 위험 | 높은 | 10.0 비판적인 |
| 영향 | 비판적인 | |
| 있을 수 있는 일 | 가능성이 매우 높다 | |
| 호스트 체하는 | 192.168.110.14 192.168.110.60 | |

| 세부 |
|---|
| 컴퓨터 192.168.110.14 및 192.168.110.60은 둘 다 VNC(가상 네트워크 컴퓨팅, 데스크톱 공유 프로그램) 암호 및 회사 내부 네트워크에 대한 액세스와 같은 중요한 자격 증명이 포함된 단순 일반 텍스트 파일을 호스팅했습니다. |
| 이러한 시스템에 대한 읽기 액세스 권한을 획득한 제3자에게 중요한 정보에 대한 액세스 권한이 부여되고 거의 또는 전혀 노력하지 않고 외부에서 데이터를 변경할 수 있는 기능이 부여되므로 이는 엄청난 보안 위험입니다. |

| 복제 |
|--|
| 머신 192.168.110.60의 /home/.ssh에는 다음 파일이 포함되어 있습니다. |
| <pre>rvapthosting.com\josh: [REDACTED] [Our domain - rvapthosting.com] [My comp] 192.168.120.20:22 ~</pre> |
| 머신 192.168.110.60은 ".things"라는 홈 디렉토리의 숨겨진 폴더와 "hosts"라는 다른 폴더에 다음 파일을 포함하고 있습니다. |

```
Passwd for Bob
- Make sure to do routine cleanup on his desktop after he leaves work
- Make sure to update his personal computer whenever he takes vacation

rvapthosting.com\bob: [REDACTED]

# Powershell oneliner for access bob's workstation
enter-pssession -computer 192.168.120.18 -credentials rvapthosting.com\bob
enter-pssession -computer bob.rvapthosting.com -credentials rvapthosting.com\bob

# RDP

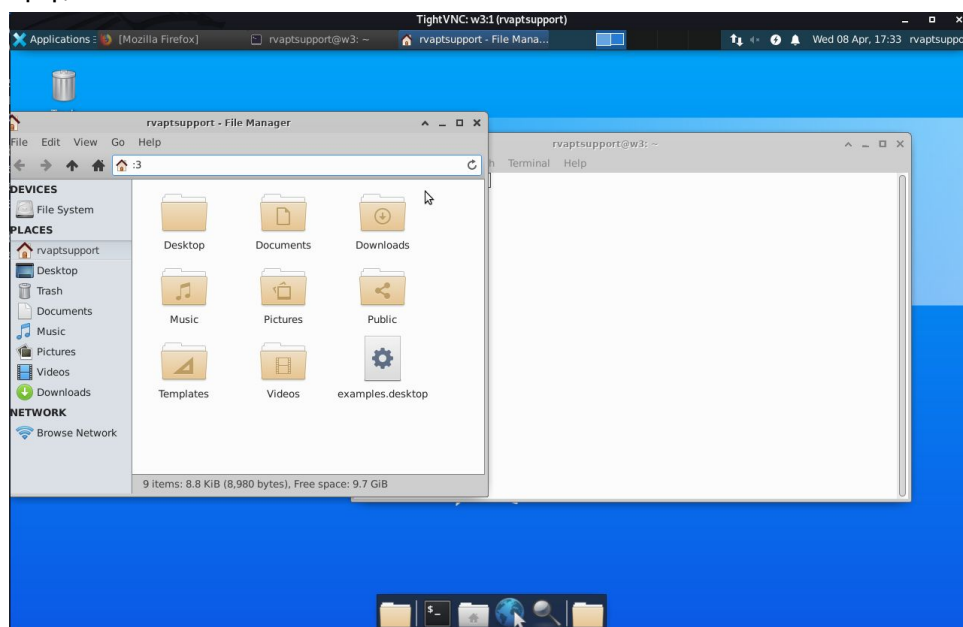
# PSexec
```

```
[ftp]
josh: [REDACTED]

[bob]
- FTP server

[joe]
- Local Admin, np
```

머신 192.168.110.14에는 VNC 서비스에 대한 액세스를 허용하는 홈 디렉토리의 'vnc.txt'도 포함되어 있습니다.



완화

암호와 같은 민감한 정보는 컴퓨터에 암호화되지 않은 상태로 저장되어서는 안 됩니다. 그러나 이것은 또한 직원들이 암호를 기억하는 데 어려움을 겪는 문제를 나타내는 것으로 보입니다. 보다 안전한 암호 검색 방법은 Bitwarden 또는 Lastpass와 같은 암호 관리자를 통합하는 것입니다.

참조

<https://bitwarden.com/>

<https://www.lastpass.com/solutions/business-password-manager>

| # 2 - 인증되지 않은 MYSQL | | CVSS |
|---------------------|----------------|----------------------------|
| 위험 | 높은 | 10.0 비판적인 |
| 영향 | 중요한 | |
| 있을 수 있는 일 | 가능성이 매우 높다 | |
| 호스트 체하는 | 192.168.110.20 | |

| 세부 |
|--|
| <p>MySQL은 일반적으로 데이터를 안전하게 유지하기 위해 사용자 이름과 비밀번호로 설정됩니다. 그러나 기본적으로 비밀번호 없이 사용자 이름 "root"로 데이터베이스에 액세스할 수 있습니다. 이것은 일반적으로 무단 액세스를 방지하기 위해 비활성화됩니다.</p> <p>192.168.110.20에는 기본 루트 액세스 권한이 있는 MySQL 인스턴스가 있어 데이터베이스와 직접 상호 작용할 수 있습니다. 머신도 MySQL을 노출했다는 사실과 결합하여 자격 증명 없이 MySQL 데이터베이스에서 원격으로 명령을 실행할 수 있었습니다.</p> <p>이것은 사용자 이름, 암호, 회사 데이터 및 개인 정보와 같은 데이터가 MySQL 데이터베이스에 저장될 수 있고 이와 같은 데이터에 대한 무료 액세스는 잠재적으로 파괴적일 수 있으므로 매우 위험한 취약점입니다.</p> |

| 복제 |
|--|
| <p>이 특정 MySQL 데이터베이스가 인터넷에 노출되었기 때문에 -u 옵션을 사용하여 루트로 액세스할 수 있었습니다.</p> <pre> c0nfusedk-king@kali:~/RVAPT/external/host-20\$ mysql -h 192.168.110.20 -u root Welcome to the MariaDB monitor. Commands end with ; or \g. Your MySQL connection id is 1143 Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu) Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. MySQL [(none)]> </pre> |

완화

MySQL에서는 기본적으로 사용자 이름이 root이며 암호가 필요하지 않습니다. 이 사용자는 다른 사용자가 추가될 때 활성화된 상태로 유지됩니다. 이 문제를 제거하려면 루트 사용자가 강제 암호를 활성화해야 합니다.

참조

해당 없음

| # 3 - 침해 지표 | | CVSS |
|-------------|--|--------------------------|
| 위험 | 높은 | 해당 없음 비판적인 |
| 영향 | 중요한 | |
| 있을 수 있는 일 | 가능성이 매우 높다 | |
| 호스트 체하는 | 192.168.110.10 192.168.110.12 192.168.110.14 | |

| 세부 |
|---|
| legionminer_callbak은 외부 네트워크의 여러 호스트에서 발견되었으며, 이는 제3자가 자체 목적을 위해 사용하지 않는 컴퓨팅 성능을 활용하기 위해 각 장치에 암호화폐 채굴기를 설치한 증거를 보여줍니다. |
| 광부가 CPU 전력을 사용하면 각 시스템의 효율성이 크게 느려지고 다른 하드웨어 오작동으로 이어질 수 있으므로 이것이 네트워크에 미칠 수 있는 영향은 큼니다. |

| 복제 |
|--|
| Legionminer_callbak는 /home/rvaptsupport 디렉토리 또는 192.168.110.60의 /home/josh에 있는 모든 외부 네트워크 시스템에서 찾을 수 있습니다. |

```

root@s1:/home/sysadminjosh# ls -la
total 7392
drwxr-xr-x 7 sysadminjosh sysadminjosh 4096 Apr  5 19:43 .
drwxr-xr-x 5 root          root          4096 Apr  5 18:51 ..
-rw----- 1 sysadminjosh sysadminjosh 2379 Apr  5 20:19 .bash_history
-rw-r--r-- 1 sysadminjosh sysadminjosh  220 Sep 12  2018 .bash_logout
-rw-r--r-- 1 sysadminjosh sysadminjosh 3771 Sep 12  2018 .bashrc
drwx----- 4 sysadminjosh sysadminjosh 4096 Feb 22 22:17 .cache
drwx----- 3 sysadminjosh sysadminjosh 4096 Feb 22 22:17 .config
-rw-r--r-- 1 sysadminjosh sysadminjosh 8980 Apr 16  2018 examples.desktop
drwx----- 3 sysadminjosh sysadminjosh 4096 Feb 14 23:34 .gnupg
-rwxr-xr-x 1 sysadminjosh sysadminjosh 7496474 Apr  5 18:49 .legionminer_callbak
drwx----- 5 sysadminjosh sysadminjosh 4096 Feb 22 22:17 .mozilla
-rw-r--r-- 1 sysadminjosh sysadminjosh  807 Sep 12  2018 .profile
drwx----- 3 sysadminjosh sysadminjosh 4096 Apr  5 17:47 .ssh
-rw-r--r-- 1 sysadminjosh sysadminjosh    0 Feb 14 20:43 .sudo_as_admin_successful
-rw----- 1 sysadminjosh sysadminjosh 7655 Apr  5 19:43 .viminfo
-rw----- 1 sysadminjosh sysadminjosh  48 Feb 22 22:16 .Xauthority
root@s1:/home/sysadminjosh#

```

완화

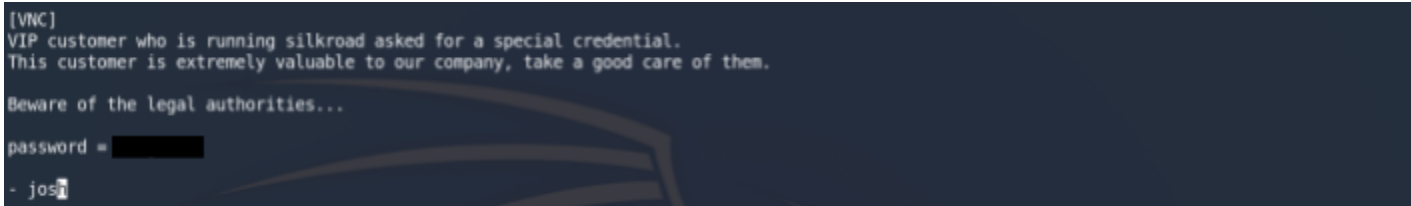
보다 강력한 침입 탐지 시스템을 구현하고 이미 시스템에 있는 기존 크립토재킹 소프트웨어를 제거합니다.

참조

해당 없음

| # 4 - 관리자 허용 외부 액세스 | | CVSS |
|---------------------|----------------|----------------------|
| 위험 | 높은 | 해당 없음 비판적인 |
| 영향 | 비판적인 | |
| 있을 수 있는 일 | 가능성이 매우 높다 | |
| 호스트 체하는 | 192.168.110.60 | |

| 세부 |
|---|
| 192.168.110.60에는 시스템 관리자인 Josh가 외부 "VIP" 고객에게 주요 VNC 자격 증명을 제공했음을 나타내는 파일이 포함되어 있습니다. 키 자격 증명은 일반 대중에게 공개하는 것과 같기 때문에 회사 외부에서 절대 공유해서는 안 됩니다. 특히 자격 증명을 얻은 사용자가 불법 활동을 저지르고 있는 것으로 보이기 때문에 이는 엄청난 보안 위험입니다. 이는 결국 RVAPT 호스팅에 중대한 법적 영향을 미칠 수 있습니다. |

| 복제 |
|--|
| 이에 대한 증거는 192.168.110.60의 루트 디렉토리에서 찾을 수 있습니다.  |

| 완화 |
|--|
| 이 시스템과 관련된 암호를 즉시 변경하고 Josh의 관리 자격 증명을 제거하십시오. |

| 참조 |
|---|
| https://www.wikihow.com/Fire-an-Employee-Compassionately |

| # 5 - SMBV1 활성화됨 | | CVSS |
|------------------|--|-------------|
| 위험 | 중간 높음 | 9.3 비판적인 |
| 영향 | 중요한 | |
| 있을 수 있는 일 | 할 것 같은 | |
| 호스트 체하는 | 192.168.120.18 192.168.120.20 192.168.120.21 | |

세부

Windows의 SMBv1 서버에는 "Windows SMB 원격 코드 실행 취약점"이라는 두드러진 취약점이 있습니다. 이를 통해 원격 위치에서 코드를 실행할 수 있으며, 이 경우 암호를 쉽게 해독하는 데 사용할 수 있는 키 해시 덤프가 가능합니다.

내부 네트워크에 대한 액세스 권한을 얻을 수 있는 사람은 누구나 쉽게 관리 제어 권한을 얻을 수 있으므로 이는 시스템에 상당히 심각한 위협입니다.

복제

Active Directory 사후 공격 도구인 crackmapexec를 사용하여 AD 시스템에서 암호를 해독하는 데 사용할 수 있는 키 해시를 덤프할 수 있었습니다.

```
j0j@kali:~/Documents/heckcomp/cme$ crackmapexec smb 192.168.120.21 -u josh -p '' --sam | --sam
SMB 192.168.120.21 445 JOE [+] Windows 10 Enterprise Evaluation 18363 x64 (name:JOE) (domain:RVAPTHOSTING) (signing:False) (SMBv1:True)
SMB 192.168.120.21 445 JOE [+] RVAPTHOSTING\josh: (Pwn3d!)
SMB 192.168.120.21 445 JOE [+] Dumping SAM hashes
SMB 192.168.120.21 445 JOE Administrator:500:aad3b43...
SMB 192.168.120.21 445 JOE Guest:501:aad3b...
SMB 192.168.120.21 445 JOE DefaultAccount:503:aad3b...
SMB 192.168.120.21 445 JOE WDAGUtilityAccount:504:aad3b...
SMB 192.168.120.21 445 JOE Winlog-1:1001:aad3b43f...
SMB 192.168.120.21 445 JOE Winlog-2:1003:aad3b43f...
SMB 192.168.120.21 445 JOE Winlog-3:1005:aad3b43f...
SMB 192.168.120.21 445 JOE [+] Added 7 SAM hashes to the database

j0j@kali:~/Documents/heckcomp/cme$ crackmapexec smb 192.168.120.21 -u joe -p '' --local-auth --local-auth=NTLM
SMB 192.168.120.21 445 JOE [...] Windows 10 Enterprise Evaluation 18363 x64 (name:JOE) (domain:RVAPTHOSTING) (signing:False) (SMBv1:True)
SMB 192.168.120.21 445 JOE [+] RVAPTHOSTING\josh: (Pwn3d!)
SMB 192.168.120.21 445 JOE [+] Dumping LSA secrets
SMB 192.168.120.21 445 JOE RVAPTHOSTING.CM/joe:$OCC2
SMB 192.168.120.21 445 JOE RVAPTHOSTING.COM/Administrator:$OCC
SMB 192.168.120.21 445 JOE RVAPTHOSTING.COM/builder:$OCC
SMB 192.168.120.21 445 JOE RVAPTHOSTING.COM/job:$OCC
SMB 192.168.120.21 445 JOE RVAPTHOSTING.COM/josh:$OCC2
SMB 192.168.120.21 445 JOE RVAPTHOSTING\JOE$aes256
SMB 192.168.120.21 445 JOE RVAPTHOSTING\JOE$aes128
SMB 192.168.120.21 445 JOE RVAPTHOSTING\JOE$des
SMB 192.168.120.21 445 JOE RVAPTHOSTING\JOE$aesN
SMB 192.168.120.21 445 JOE dcsapi_machinkey:B4
j0j@_userkey:Red
SMB 192.168.120.21 445 JOE NLSAM:
SMB 192.168.120.21 445 JOE [+] Dropped LS LSA secrets to /home/j0j/.cme/logs/XOE-192.168.120.21-2020-04-16.193651.lsa and /home/j0j/.cme/logs/XOE-192.168.120.21-2020-04-16.193651.cached
```

완화

현재 SMB의 각 버전에는 주목할만한 취약점이 있습니다. 따라서 완화를 위한 최선의 과정은 SMB의 각 버전과 관련 패치를 조사하여 RVAPT 호스팅의 요구 사항에 가장 적합한 솔루션을 선택하는 것입니다.

참조

<https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3>

<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/smbghost-cve-020-0796-a-critical-smbv3-rce-vulnerability/>

| # 6 - 노출된 MYSQL | | CVSS |
|-----------------|----------------------------------|------------------------------|
| 위험 | 중간 | <div>8.3</div> <div>높은</div> |
| 영향 | 보통의 | |
| 있을 수 있는 일 | 할 것 같은 | |
| 호스트 체하는 | 192.168.110.10 192.168.110.20 | |

| 세부 |
|--|
| <p>MySQL은 일반적으로 중요한 데이터를 저장하는 데 사용되기 때문에 일반적으로 인프라 내부에 보관됩니다. 그러나 외부 네트워크에 MySQL이 노출되어 있으면 외부의 모든 머신이 접속할 수 있으며 자격 증명을 획득하거나 악용할 경우 외부의 모든 머신이 데이터베이스의 데이터에 액세스하거나 변경할 수 있습니다.</p> <p>노출된 데이터베이스를 사용하면 내부 네트워크 외부에서 잠재적으로 민감한 데이터에 액세스하는 것이 매우 쉬워질 수 있기 때문에 이 발견의 영향은 큼니다.</p> |

| 복제 |
|--|
| <p>인터넷에 노출되어 있기 때문에 이 취약점을 복제하는 것은 원격으로 MySQL에 연결하는 것만큼 간단합니다.</p> <pre> c0nfusedk-king@kali:~/RVAPT/external/host-20\$ mysql -h 192.168.110.20 -u root Welcome to the MariaDB monitor. Commands end with ; or \g. Your MySQL connection id is 1143 Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu) Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. MySQL [(none)]> </pre> |

완화

애플리케이션에 사용되는 내부 데이터베이스는 외부 인터페이스를 통해 외부 세계에 노출되어서는 안 됩니다. 이는 공격자에게 침입하여 중요한 정보를 훔칠 수 있는 기회를 제공합니다. 이를 완화하려면 네트워크의 다른 호스트에서 필요한 경우 localhost 인터페이스 또는 내부 인터페이스를 사용하도록 SQL 데이터베이스의 구성을 변경해야 합니다. 또한 이러한 데이터베이스에 연결하는 웹 서비스는 사용하는 인터페이스도 변경해야 합니다.

참조

해당 없음

| # 7 - MINISERV 원격 코드 실행 | | CVSS |
|-------------------------|----------------|------------------------------|
| 위험 | 높은 | <div>8.2</div> <div>높은</div> |
| 영향 | 중요한 | |
| 있을 수 있는 일 | 가능성이 매우 높다 | |
| 호스트 체하는 | 192.168.110.60 | |

| 세부 |
|---|
| <p>Webmin은 관리자가 Linux 서버를 관리할 수 있도록 하는 웹 응용 프로그램이며 Webmin 웹 응용 프로그램을 처리하는 Miniserv라는 웹 서버 응용 프로그램을 사용합니다.</p> <p>192.168.110.60에서 사용 중인 Webmin 버전은 취약한 것으로 악명 높은 서비스인 Miniserv 1.92를 사용합니다. 공개적으로 사용 가능한 익스플로잇을 사용하여 Miniserv의 취약점을 사용하여 원격으로 명령을 실행할 수 있습니다.</p> <p>다른 원격 코드 실행 익스플로잇과 마찬가지로 외부 소스가 시스템의 시스템에 액세스하면 잠재적으로 심각한 피해를 입힐 수 있기 때문에 회사에 상당한 위험을 초래합니다.</p> |

| 복제 |
|--|
| <p>Webmin 1.92의 취약점은 잘 문서화되어 있으며 CVE(Common Vulnerability & Exposure) 코드는 CVE-2019-15107입니다. 서비스를 호스팅하는 포트에서 실행하기만 하면 되는 공개적으로 사용 가능한 Python 스크립트가 있습니다.</p> <pre> c0nfusedk-king@kali:~/RVAPT/external/host-60/code\$./CVE_2019_15107.py http://192.168.110.60:10000 whoami </pre>  <pre> vuln_url= http://192.168.110.60:10000/passwd_change.cgi Command Result = root </pre> |

완화

이 악용을 완화하기 위해 RVAPT Hosting은 애플리케이션의 최신 버전으로 업데이트하거나 유사한 애플리케이션을 찾아야 합니다.

참조

<https://github.com/jas502n/CVE-2019-15107> <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15107>

| # 8 - 루트 실행 애플리케이션 | | CVSS |
|--------------------|----------------|------------------------------|
| 위험 | 중간 높음 | <div>8.2</div> <div>높은</div> |
| 영향 | 중요한 | |
| 있을 수 있는 일 | 할 것 같은 | |
| 호스트 체하는 | 192.168.110.60 | |

| 세부 |
|--|
| <p>Linux 장치의 루트 사용자는 실행할 수 있는 명령에 제한 없이 시스템에 대한 완전한 액세스 권한이 있는 사용자입니다. 이러한 이유로 루트 사용자로부터 모든 종류의 응용 프로그램을 실행하는 것은 나쁜 습관입니다. 모든 취약점이 시스템에서 가장 높은 수준의 코드 실행에 영향을 미칠 수 있기 때문입니다. 예를 들어 루트에 있는 응용 프로그램을 통해 실행되는 원격 코드 실행은 시스템에서 모든 루트 명령을 실행할 수 있습니다.</p> <p>RVAPT는 192.168.110.60에서 루트로 Miniserv 1.92를 호스팅하고 있습니다. 이는 공격에 사용한 익스플로잇이 루트 명령을 실행할 수 있음을 의미합니다.</p> |

| 복제 |
|--|
| <p>앞서 언급한 Webmin 취약점으로 인해 192.168.110.60에서 루트 명령을 실행할 수 있었습니다.</p> <pre> c0nfusedk-king@kali:~/RVAPT/external/host-60/code\$./CVE_2019_15107.py http://192.168.110.60:10000 whoami CVE_2019_15107 python By jas502n vuln_url= http://192.168.110.60:10000/password_change.cgi Command Result = root </pre> |

완화

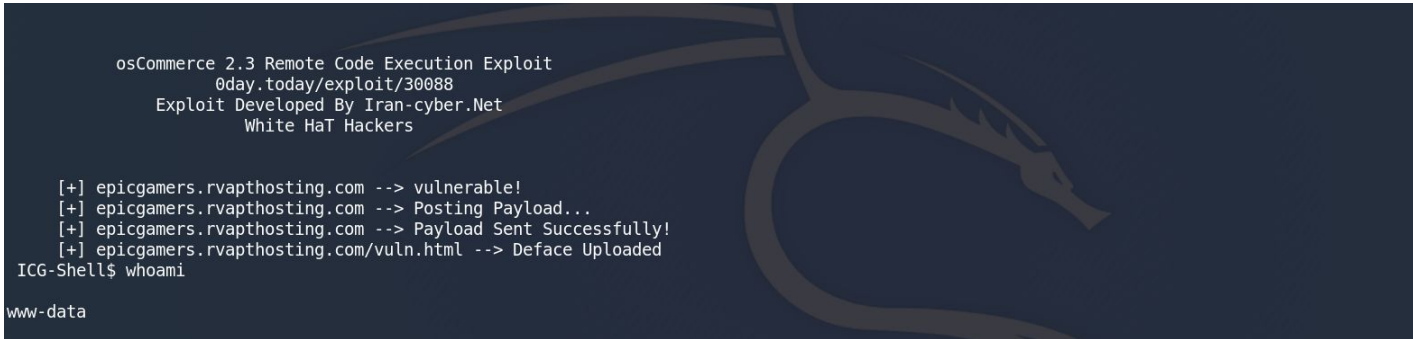
응용 프로그램은 가능한 최소한의 권한으로 실행되어야 하며 절대적으로 필요한 경우에만 더 많은 권한을 부여해야 합니다. 이를 완화하는 데는 다른 사용자(일반적으로 www-data)가 실행할 애플리케이션을 마이그레이션하면 되므로 시간이 거의 걸리지 않습니다.

참조

해당 없음

| # 9 - OSCOMMERCE 원격 코드 실행 | | CVSS |
|---------------------------|----------------|------------------------------|
| 위험 | 높은 | <div>7.2</div> <div>높은</div> |
| 영향 | 중요한 | |
| 있을 수 있는 일 | 가능성이 매우 높다 | |
| 호스트 체하는 | 192.168.110.10 | |

| 세부 |
|---|
| <p>OsCommerce는 epicgamers.rvaphosting.com과 같은 온라인 상점 또는 서비스를 호스팅하는 웹 서버에서 사용되는 오픈 소스 온라인 상점 관리 소프트웨어입니다. epicgamers(2.3)에서 사용되는 특정 버전의 OsCommerce는 외부 공격에 취약합니다. 쉽게 사용할 수 있는 익스플로잇을 사용하면 웹 서버에 대한 원격 실행 액세스 권한을 얻을 수 있습니다. 이를 통해 컴퓨터에서 파일을 보는 데 사용할 수 있는 대화형 셸이 허용됩니다.</p> <p>이는 제한된 셸에서 충분한 시간이 궁극적으로 더 큰 시스템에 대한 액세스로 이어질 수 있는 더 깊은 수준의 악용으로 이어질 수 있으므로 인프라에 잠재적으로 큰 영향을 미칠 수 있습니다.</p> |

| 복제 |
|--|
| <p>Metasploit이라는 익스플로잇 및 취약성 검증 도구를 사용하여 osCommerce 2.3에 대한 일반적인 익스플로잇을 찾고 192.168.110.10에서 이를 호스팅하는 포트에 페이로드를 보낼 수 있었습니다. 이것은 RCE를 허용했습니다.</p> |
|  <pre> osCommerce 2.3 Remote Code Execution Exploit 0day.today/exploit/30088 Exploit Developed By Iran-cyber.Net White HaT Hackers [+] epicgamers.rvaphosting.com --> vulnerable! [+] epicgamers.rvaphosting.com --> Posting Payload... [+] epicgamers.rvaphosting.com --> Payload Sent Successfully! [+] epicgamers.rvaphosting.com/vuln.html --> Deface Uploaded ICG-Shell\$ whoami www-data </pre> |

완화

OSCommerce는 클라이언트 응용 프로그램이므로 최선의 조치는 적절한 클라이언트에 연락하여 이 보안 취약점을 알리는 것입니다. 인프라에서 이 취약점을 방지할 수 있는 업데이트된 OSCommerce 버전이 있습니다.

참조

<https://github.com/04x/OsCommerce2-3RceExploit>
<https://nvd.nist.gov/vuln/detail/CVE-2018-18572>
<https://github.com/osCommerce>

| # 10 - 로컬 관리자 자격 증명 재사용 | | CVSS |
|-------------------------|--|------------------------------|
| 위험 | 중간 | <div>7.2</div> <div>높은</div> |
| 영향 | 보통의 | |
| 있을 수 있는 일 | 가능한 | |
| 호스트 체하는 | 192.168.120.18 192.168.120.20 192.168.120.21 | |

| 세부 |
|---|
| <p>로컬 관리자 계정은 계정 t로 관리자 업무를 수행하는 데 사용됩니다.</p> <p>티 卜</p> <div> <div>SMB</div> <div>192.168.120.18</div> <div>445</div> <div>BOB</div> <div>[+] BOB\Administrator b0d77d4966a5aa4c5145ee601d5f18df (Pwn3d!)</div> </div> <div> <div>SMB</div> <div>192.168.120.2</div> <div>445</div> <div>FTP</div> <div>[+] FTP\Administrator b0d77d4966a5aa4c5145ee601d5f18df STATUS_LOGON_FAILURE</div> </div> <div> <div>SMB</div> <div>192.168.120.21</div> <div>445</div> <div>JOE</div> <div>[+] JOE\Administrator b0d77d4966a5aa4c5145ee601d5f18df (Pwn3d!)</div> </div> <div> <div>SMB</div> <div>192.168.120.1</div> <div>445</div> <div>DC</div> <div>[+] DC\Administrator b0d77d4966a5aa4c5145ee601d5f18df STATUS_LOGON_FAILURE</div> </div> <div> <div>SMB</div> <div>192.168.120.20</div> <div>445</div> <div>JOSH</div> <div>[+] JOSH\Administrator b0d77d4966a5aa4c5145ee601d5f18df (Pwn3d!)</div> </div> |

| 복제 |
|------------------|
| <div>해당 없음</div> |

| 완화 |
|--|
| <p>컴퓨터에 대한 지원을 관리할 때 업데이트를 수행할 관리자 계정이 있는 것이 좋지만 로컬 관리자 계정은 컴퓨터 수준 계정이므로 공유 암호가 없어야 합니다. 도메인 관리자 계정 또는 다른 암호를 사용하는 로컬 관리자 계정에서 관리를 수행해야 합니다. 제안된 완화 방법은 로컬 관리자 계정에 대해 다른 암호를 생성하거나 도메인 계정을 위해 암호를 비활성화하는 것입니다.</p> |

| 참조 |
|------------------|
| <div>해당 없음</div> |

| # 11 - SMB에서 호스팅되는 C:\WINDOWS 폴더 | | CVSS |
|----------------------------------|----------------|-----------|
| 위험 | 중간 | 6.3 중간 |
| 영향 | 보통의 | |
| 있을 수 있는 일 | 할 것 같은 | |
| 호스트 체하는 | 192.168.120.20 | |

| 세부 |
|--|
| C:\Windows는 전체 OS의 초기 디렉토리입니다. 따라서 머신의 파괴를 방지하기 위해 이 디렉토리를 보호하는 것이 매우 중요합니다. 192.168.120.20은 네트워크에서 이 디렉토리를 호스팅하므로 동일한 네트워크에 있는 모든 사용자가 액세스할 수 있습니다. 이는 악의적인 사용자가 OS의 내부 파일에 액세스할 수 있으므로 매우 위험합니다. |

| 복제 |
|--|
| 내부 네트워크에 연결하고 네트워크 탭을 연 다음 192.168.120.20(JOSH)으로 이동합니다. |

| 완화 |
|---|
| 내부 파일 시스템의 가능한 손상을 완화하기 위해 RVAPT Hosting이 내부 네트워크에서 공유 파일 권한 설정을 간소화하는 것이 좋습니다. |

| 참조 |
|-------|
| 해당 없음 |

| # 12 - FTP 익명 로그인 | | CVSS |
|-------------------|----------------|------------------------------|
| 위험 | 중간 | <div>5.3</div> <div>중간</div> |
| 영향 | 미성년자 | |
| 있을 수 있는 일 | 가능성이 매우 높다 | |
| 호스트 체하는 | 192.168.110.60 | |

| 세부 |
|---|
| <p>FTP(파일 전송 프로토콜)는 일반적으로 서버에서 파일을 보내고 받기 위해 인증이 필요합니다. 그러나 서버는 모든 사용자가 액세스할 수 있도록 익명 로그인을 설정할 수 있습니다.</p> <p>중요한 데이터가 있는 장치에 공개 익명 FTP 로그인이 있는 경우 회사에 특히 위험할 수 있습니다. 타사가 호스트의 모든 파일에 직접 액세스할 수 있기 때문입니다.</p> |

| 복제 |
|--|
| <p>포트 192.168.110.60에서 ftp에 연결되면 사용자 이름으로 anonymous를 입력하고 서버에 액세스할 수 있는 암호 아무 것도 입력합니다.</p> <p>보시다시피 anonymous_enable이 YES로 설정되어 있습니다.</p> <pre> listen=YES anonymous_enable=YES local_enable=YES write_enable=YES dirmessage_enable=YES use_localtime=YES xferlog_enable=YES connect_from_port_20=YES #secure_chroot_dir=/var/run/vsftpd/empty pam_service_name=vsftpd rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key ssl_enable=NO write_enable=YES anon_upload_enable=YES local_root=/ftp anon_umask=022 anon_root=/ftp allow_writeable_chroot=YES </pre> |

완화

FTP 서버에서 익명 로그인을 비활성화하는 것은 vsftpd.conf 파일(일반적으로 /etc/vsftpd/vsftpd.conf)에서 anonymous_enable을 NO로 설정하기만 하면 됩니다.

참조

해당 없음

| # 13 - 해체된 FTP 서버 | | CVSS |
|-------------------|---------------|-----------|
| 위험 | 낮음 중간 | 5.3 중간 |
| 영향 | 미성년자 | |
| 있을 수 있는 일 | 할 것 같은 | |
| 호스트 체하는 | 192.168.120.2 | |

| 세부 |
|---|
| 192.168.120.2는 이전에 ftp 서버로 사용되었습니다. 그러나 폐기되었으며 사용하지 않을 예정이었습니다. 그럼에도 불구하고 서버는 여전히 실행 중이며 중요한 회사 데이터가 포함되어 있습니다. |
| 서버가 여전히 암호로 보호되어 있기 때문에 이것은 즉각적인 위험은 아니지만 일단 해당 서버의 파일이 크랙되면 CEO를 포함하여 내부 네트워크에서 더 많은 시스템을 손상시킬 수 있을 만큼 중요합니다. |

| 복제 |
|--|
| 192.168.120.2에서 ftp 서버에 연결합니다. 여전히 파일을 업로드하고 파일을 다운로드할 수 있습니다. |

| 완화 |
|---|
| 이 서버는 폐기되었으므로 계속 실행할 필요가 없으므로 가능한 한 빨리 FTP 서비스를 종료해야 합니다. |

| 참조 |
|-------|
| 해당 없음 |

| # 14 - 안전하지 않은 HTTP | | CVSS |
|---------------------|--|------------------------------|
| 위험 | 낮은 | <div>2.6</div> <div>낮은</div> |
| 영향 | 무시할 수 있는 | |
| 있을 수 있는 일 | 가능한 | |
| 호스트 체하는 | 192.168.110.10 192.168.110.12 192.168.110.14 192.168.110.60 | |

| 세부 |
|--|
| <p>HTTPS는 컴퓨터와 웹 사이트 간에 데이터를 전송하기 위해 암호화를 사용하는 보다 안전한 HTTP 버전입니다. 표준 HTTP를 사용하면 제3자가 로그인 정보, 중요한 회사 데이터, 개인 정보 등을 포함할 수 있는 오픈 소스 소프트웨어를 사용하여 네트워크를 통해 전송된 데이터를 가로챌 수 있습니다.</p> |

| 복제 |
|--|
| <p>호스팅 중인 웹사이트를 열고 보안 인증서 또는 URL 왼쪽의 자물쇠 아이콘을 확인합니다.</p> |

| 완화 |
|--|
| <p>웹사이트가 HTTP를 사용할 특별한 이유가 없으므로 RVAPT Hosting에서 보안을 강화하기 위해 웹사이트에 대한 SSL 인증서 구매를 검토하는 것이 좋습니다.</p> |

| 참조 |
|------------------|
| <div>해당 없음</div> |

| # 15 - BRICKTUBE 원격 코드 실행 | | CVSS |
|---------------------------|----------------|------------------------------|
| 위험 | 없음 | <div>0.0</div> <div>정보</div> |
| 영향 | 중간 | |
| 있을 수 있는 일 | 없음 | |
| 호스트 체하는 | 192.168.110.20 | |

| 세부 |
|---|
| <p>192.168.110.20에서 호스팅되는 Bricktube 웹사이트가 잠재적으로 악용될 수 있습니다. 작동하지 않는 동안 시스템에 대한 액세스 권한을 얻은 후 소스 코드를 검사한 결과 웹 사이트의 보안 위험이 드러났습니다. 웹 사이트가 가동되면 악용될 가능성이 매우 높고 원격 코드 실행이 허용됩니다.</p> |

| 복제 |
|---|
| <p>192.168.110.20에서 Bricktube 사이트의 소스 코드를 조사하십시오. 여기에는 악용하기 매우 쉬운 수많은 취약점이 포함되어 있습니다.</p> |

| 완화 |
|---|
| <p>보다 안전한 웹사이트를 만들고 인프라의 보안을 유지하기 위해 일시적으로 웹사이트를 폐쇄하고 고객에게 연락하는 것이 가장 좋습니다.</p> |

| 참조 |
|------------------|
| <div>해당 없음</div> |