컴퓨터 컴퓨터 이름 또는 NULL 사용자 이름이 액세스 로그에 로깅되는 이유는 무엇입니까?

목차

질문

- 컴퓨터 컴퓨터 이름 또는 NULL 사용자 이름이 액세스 로그에 로깅되는 이유는 무엇입니까?
- 나중에 인증 면제를 위해 워크스테이션 또는 NULL 자격 증명을 사용하여 요청을 어떻게 식별합니까?

환경

- Cisco WSA(Web Security Appliance) - 모든 버전
- IP 서로게이트를 사용하는 인증 체계 NTLMSSP
- Windows Vista 및 최신 데스크톱 및 모바일 Microsoft 운영 체제

증상

WSA는 일부 사용자의 요청을 차단하거나 예기치 않게 동작합니다.
액세스 로그는 사용자 ID 대신 컴퓨터 시스템 이름 또는 NULL 사용자 이름 및 도메인을 표시합니다
.

이 문제는 다음 후에 해결됩니다.

- 서로게이트 시간 초과(서로게이트 시간 제한의 기본값은 60분)
- 프록시 프로세스 재시작(CLI 명령 > *진단* > *프록시* > *kick*)
- 인증 캐시 플러싱(CLI 명령 > *authcache* > *flushall*)

배경 정보

최신 버전의 Microsoft 운영 체제에서는 응용 프로그램에서 더 이상 인터넷으로 요청을 보낼 때 실제 사용자가 로그인하지 않아도 됩니다.이러한 요청이 WSA에 의해 수신되고 인증하도록 요청되면 클라이언트 워크스테이션에서 인증에 사용할 수 있는 사용자 자격 증명이 없습니다. 클라이언트 워크스테이션은 대신 컴퓨터의 시스템 이름을 대체용으로 사용할 수 있습니다.

WSA는 제공된 시스템 이름을 가져와 AD(Active Directory)에 전달하여 이를 검증합니다.

유효한 인증으로 WSA는 시스템의 워크스테이션 이름을 워크스테이션의 IP 주소에 바인딩하는 IP 서로게이트를 생성합니다.동일한 IP에서 추가 요청이 수신되면 서로게이트를 사용하여 워크스테이션 이름을 사용합니다.

워크스테이션 이름이 AD 그룹의 구성원이 아닌 경우 요청이 예상 액세스 정책을 트리거하지 못하여 차단될 수 있습니다.이 문제는 서로게이트가 시간 초과되어 인증을 갱신해야 할 때까지 계속됩니다.이번에는 실제 사용자가 로그인하고 유효한 사용자 자격 증명을 사용할 수 있는 상태에서 이 정보를 사용하여 새 IP 서로게이트가 생성되고 추가 요청이 예상 액세스 정책과 일치합니다.

응용 프로그램이 잘못된 자격 증명(NULL 사용자 이름 및 NULL 도메인)을 전송하고 유효한 컴퓨터 자격 증명을 전송하지 않는 경우도 있습니다.이는 인증 실패로 간주되며 차단되거나 게스트 정책이 활성화된 경우 실패한 인증은 "게스트"로 간주됩니다.

워크스테이션 이름은 **$DOMAIN**으로 끝납니다. 이를 통해 **$@**에 대한 액세스 로그에서 CLI 명령 grep를 사용하여 워크스테이션 이름을 쉽게 추적할 수 있습니다.자세한 내용은 아래 예를 참조하십시오.

```
> grep $@ accesslogs

1332164800.0000 9 10.20.30.40 TCP_DENIED/403 5608 GET http://www.someURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_WEBCAT_11-DefaultGroup-Internet-NONE-NONE-
NONE-NONE <-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

위 줄은 IP 주소 10.20.30.40 및 시스템 이름 gb0000d01$에 대해 이미 생성된 IP Surrogate의 예를 보여줍니다.

시스템 이름을 보낸 요청을 찾으려면 특정 IP 주소에 대한 워크스테이션 이름의 첫 번째 발생을 파악해야 합니다.다음 CLI 명령은 이를 수행합니다.

```
> grep 10.20.30.40 -p accesslogs
```

워크스테이션 이름의 첫 번째 항목에 대한 결과를 검색합니다. 세 개의 첫 번째 요청은 여기에 설명된 대로 아래 예와 같이 일반적으로 NTLM Single-Sin(NTLMSSP/NTLMSSP) 핸드셰이크로 인식됩니다.

```
1335248044.836 0 10.20.30.40 TCP_DENIED/407 1733 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.839 0 10.20.30.40 TCP_DENIED/407 483 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.845 10 10.20.30.40 TCP_DENIED/403 2357 GET http://SomeOtherURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_ADMIN_PROTOCOL_11-DefaultGroup-DefaultGroup-
DefaultGroup-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

문제를 해결할 때 이러한 요청이 동일한 URL에 대한 요청이고 자동 NTLMSSP 핸드셰이크임을 나타내는 매우 짧은 시간 간격으로 기록되었는지 확인합니다.

위의 예에서, 명시적 요청에 대한 이전 요청은 HTTP 응답 코드 407(Proxy Authentication required)으로 기록되고, 투명 요청은 HTTP 응답 코드 401(Unauthenticated)으로 기록됩니다.

AsyncOS 7.5.0 이상에서는 머신 자격 증명에 대해 다른 서로게이트 시간 제한을 정의할 수 있는 새로운 기능을 사용할 수 있습니다.다음 명령을 사용하여 구성할 수 있습니다.

```
> advancedproxyconfigChoose a parameter group:- AUTHENTICATION - Authentication
related parameters- CACHING - Proxy Caching related parameters- DNS - DNS related
parameters- EUN - EUN related parameters- NATIVEFTP - Native FTP related parameters-
FTPOVERHTTP - FTP Over HTTP related parameters- HTTPS - HTTPS related parameters-
SCANNING - Scanning related parameters- WCCP - WCCPv2 related parameters-
MISCELLANEOUS - Miscellaneous proxy relatedparameters[]> AUTHENTICATION...Enter the
surrogate timeout.[3600]>Enter the surrogate timeout for machine credentials.[10]>.
```

동일한 단계를 사용하여 어떤 요청이 NULL 자격 증명을 전송했는지 탐지하고 어떤 URL 또는 사용자 에이전트가 잘못된 자격 증명을 전송하는지 검색하고 인증에서 제외할 수 있습니다.

인증에서 URL 제외

이 요청을 통해 거짓 서로게이트가 생성되지 않도록 하려면 URL을 인증에서 제외해야 합니다.또는 URL을 인증에서 제외하는 대신 요청을 보내는 응용 프로그램을 인증에서 제외하여 인증이 면제되도록 할 수 있습니다.이는 WSA의 액세스 로그 서브스크립션에서 선택적 **사용자** 필드에 추가 매개변수 **%u**를 추가하여 액세스 로그에 로그인할 사용자 에이전트를 추가하면 가능합니다.사용자 에이전트를 식별한 후 인증에서 제외되어야 합니다.