SI 구문 분석 문제로 인한 FTD 차단 프라이빗 IP URL 문제 해결

목차

문제

FTD 디바이스는 Talos로부터 보안 인텔리전스 URL/네트워크 피드 업데이트를 수신한 후 URL 호스트에 프라이빗 IP 주소가 포함된 경우 프로덕션 내부 트래픽 차단을 시작했습니다.

영향을 받는 트래픽에는 http://10.54.1.7:8200/v1/sys/health 및 http://172.31.14.7:9100과 같은 URL이 포함됩니다. 이 트래픽은 "호스트로서 개인 IP 주소"로 분류되고 "URL Block", "blacklist", "si, force_block"과 같은 판정이 있는 Talos 관련 보안 인텔리전스 정책에 의해 차단됩니다. 이러한 행동은 내부 서비스 커뮤니케이션 및 비즈니스 운영에 영향을 미칩니다.

FTD 시스템 지원 추적을 검토할 때 다음과 같은 차단 동작이 관찰되었습니다.

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Firewall: allow rule, 'Access_Rule', allow
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Generating an EOF event with rule_id = 26845
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 SI: URL security intelligence list id 104862
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict: blacklist
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict Reason: si, force_block
```

환경

- Cisco FTD 버전 7.6.4(FMC 관리)
- URL 악의적인 카테고리로 보안 인텔리전스 피드 활성화
- URL에서 사설 IP 주소를 사용하는 내부 프로덕션 서비스
- Talos의 보안 인텔리전스 URL/네트워크 피드 업데이트 후 문제가 발생했습니다.

시스템 지원 추적 로그 이해:

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
```

- 시스템 지원 추적 로그에서 범주 값이 인쇄됩니다.
- 범주 값: [1048627]
- 범주 값과 해당 SI 피드 파일의 매핑은 FTD에서 다음 위치에서 사용할 수 있습니다.

FTD 내 위치: /ngfw/var/sf/siurl_download/url.rules

Tshoot 파일의 위치: /file-contents/var/sf/siurl_download/url.rules

<#root>

```
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$
```

cat url.rules

```
# security intelligence manifest file
si,5915d129-0d33-4e9c-969a-eab3cde32156.lf,1048589,white,any
si,ac0ef862-1cff-11ef-a575-4cf8bc134a1f.lf,1074790408,block,any
si,005056bf-1643-0ed3-0000-030068648887.lf,1048646,block,any
si,127dc4a2-1ea3-4423-a02d-1f02069828ac.lf,1048590,block,any
si,c87fe5d4-5868-11ef-8843-a8b3afb1bf74.lf,1048645,block,any
si,7c51a74a-d984-11ef-8637-e77eccc0d672.lf,1048649,block,any
si,1b117672-7453-478c-be31-b72e89ca4bfc.lf,1048616,block,any
si,2b15cb6f-a3fc-4e0e-a342-ccc5e5806394.lf,1048619,block,any
si,30f9e69c-d64c-479c-821d-0e4edab852ab.lf,1048620,block,any
si,5f8148f1-e5e4-427a-aa3b-ee1c2745f481.lf,1048623,block,any
si,8af156ca-8020-4608-9278-01b8745811b7.lf,1048626,block,any
si,d3899830-d481-4773-b4e2-7daa7acf8f75.lf,1048633,block,any
si,03709ed4-faab-47af-bade-4435f8da11f5.lf,1048615,block,any
si,bde824fd-36dd-4a7c-9cc1-80e40ac7db66.lf,1048632,block,any
si,a27c6aae-8e52-4174-a81a-47c59fecf1c3.lf,1048629,block,any
si,6ba968f4-7a25-4793-a2c8-7cc77f1f1256.lf,1048625,block,any
si,02213098-6d94-4680-8ce8-2d081638d087.lf,1048613,block,any
si,5a0b6d6b-e2c3-436f-b4a1-48248b333b57.lf,1048622,block,any
si,3e2af68e-5fc8-4b1c-b5bc-b4e7cab5c9eb.lf,1048621,block,any
si,2ccda18e-ddff-4f5c-af9a-f0098521b525.lf,1048618,block,any
si,60f4e2ab-d96c-44a0-bd38-830252b67077.lf,1048624,block,any
si,23f2a124-8278-4c03-8c9d-d28fe08b8fc9.lf,1048617,block,any
si,937cf5e8-76d1-4ba2-a83c-475dc80c6976.lf,1048628,block,any
si,032ba433-c295-11e4-a919-d4ae5275d599.lf,1048614,block,any
si,d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf,1048634,block,any
si,abdc925f-4f85-4504-90a7-c891979af648.lf,1048630,block,any
```

si,8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf,1048627,block,any >>>>>>matching category ID

```
si,b1df3aa8-2841-4c88-8e64-bfaacec71300.lf,1048631,block,any
si,ac0f6900-1cff-11ef-a575-4cf8bc134a1f.lf,1074790407,monitor,any
ac,5846a44a-3d2a-11f0-a12d-7a89a4a10ab3.lf,1048650
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$ pwd
```

이전 행을 해석하는 방법:

- 이름이 "8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf"인 파일의 콘텐츠에 범주 ID가 할당되었습니다. 1048627
- 실제 카테고리가 무엇인지 확인하려면 vi 및 임의의 편집기 툴을 사용하여 파일을 열고 카테고리의 이름이 맨 위에 표시됩니다.

<#root>

```
kkhapeka@KKHAPEKA-M-F6H2 Downloads %
```

cat -n 8c3e31be-ca41-43c8-87cb-82a35b0f5213| more

```
     1  #Cisco DNS and URL intelligence feed: URL Malicious >>>>>name of the category
     2  fadoz.metrs.workers.dev/sell/2641c1ef
     3  oauth-opensea.com
     4  account8133944-complaince.com
```

- 해당 보안 인텔리전스 피드 파일을 논리적 경로로 추적할 수 있으며, 증거 수집의 중요한 측면 중 하나는 FTD에서 로컬 시스템으로 보안 인텔리전스 피드 파일을 수동으로 다운로드하는 것입니다.
- 보안 인텔리전스 피드는 정기적으로 업데이트되며 피드 업데이트 중에는 변경 사항을 나타내는 변경 로그가 FMC 및 FTD에 없습니다.
- 보안 인텔리전스 피드를 다운로드하면 해당 시점에 피드의 스냅샷을 가져올 수 있으며 나중에 BU/TALOS에 제공할 수 있습니다.

해결

이 해결책에는 보안 인텔리전스 피드를 업데이트하고 영구 소프트웨어 수정을 기다리는 동안 임시 해결 방법을 구현하는 작업이 포함됩니다.

1단계: 보안 인텔리전스 피드 업데이트

보안 인텔리전스 피드를 업데이트하여 Talos에서 수정된 피드 콘텐츠를 가져옵니다.

FMC에서 Policies(정책) > Security Intelligence(보안 인텔리전스)로 이동하여 피드 업데이트를 수동으로 트리거하거나 자동 업데이트 주기가 완료될 때까지 기다립니다.

2단계: 임시 해결 방법 구현(문제가 지속되는 경우)

피드 업데이트 후 문제가 계속되면 영향을 받는 URL 또는 도메인을 "Do not block(차단 안 함)" 목록에 임시 해결 방법으로 추가합니다.

Policies(정책) > Security Intelligence(보안 인텔리전스)로 이동하고 URL 탭 아래의 "Do not block(차단 안 함)" 목록에 프라이빗 IP URL을 추가합니다.

3단계: URL 악성 범주 다시 활성화

피드 업데이트로 문제가 해결되었는지 확인한 후 보안 인텔리전스 컨피그레이션에 "URL 악성" 카테고리를 다시 추가합니다.

Policies(정책) > Security Intelligence(보안 인텔리전스)로 이동하고 Block List(차단 목록) 아래의 "URL Malicious(URL 악성)" 카테고리를 다시 활성화합니다.

4단계: 해결 방법 항목 제거

영구 수정이 확인되어 작동하면 영향받는 URL/도메인을 "Do not block(차단 안 함)" 목록에서 제거합니다.

5단계: 검증

이전에 영향을 받은 URL을 테스트하고 FMC에서 연결 이벤트를 모니터링하여 프라이빗 IP URL 대상이 더 이상 보안 인텔리전스에 의해 차단되지 않는지 확인합니다.

원인

이 문제는 FTD 동작에 영향을 미치는 보안 인텔리전스 피드 콘텐츠의 구문 분석 문제로 인해 발생했습니다. 보안 인텔리전스 피드에는 길이가 2047자보다 긴 URL이 있었습니다.

항목이 지원되는 길이를 초과하면 이 문제의 일부는 항목이 별도의 악성 항목으로 잘못 로드되어 관련되지 않은 트래픽을 잠재적으로 차단했기 때문일 수 있습니다. 이 동작은 Cisco 버그 ID로 추적됩니다. CSCww11335. 이 문제는 Talos 팀에서 피드 콘텐츠에 대해 수정한 수정 사항을 통해 해결되었으며, 이후 릴리스에서 가드 레일을 추가하여 향후 발생을 방지하는 영구 소프트웨어 수정이 계획되었습니다.

관련 콘텐츠

- Cisco 버그 ID: CSCw11335
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.