침입 정책에서 Sourcefire가 제공한 규칙의 기본 상태 결정

목차

소개

이 문서에서는 VRT(Vulnerability Research Team)에서 기본 침입 정책에서 규칙 상태를 결정하는 방법과 Sourcefire 어플라이언스에서 새 규칙에 대해 적절한 기본 상태를 결정하는 방법에 대해 설명합니다.

기본 정책에서 규칙 상태 결정

각 규칙에는 0개 이상의 정책 값이 있는 메타데이터 필드가 있습니다. 현재 6가지 가능한 정책 값이 있습니다.

1. 보안 ips 드롭
2. 보안 ips 알림
3. 균형 잡힌 ips 드롭
4. 균형 잡힌 ips 경고
5. 연결 IPS 드롭
6. 연결 ips 알림

IPS 정책이 Sourcefire에서 제공하는 **Balanced Security and Connectivity** 정책의 하위가 될 경우, 관리되는 디바이스는 인라인 모드에 있고, 규칙에 balanced-ips 드롭의 메타데이터 정책 값이 있을 경우, 규칙은 IPS 정책에서 이벤트를 삭제하고 생성하도록 설정됩니다. 규칙에 security-ips 드롭만 있는 정책 값이 있는 경우 정책에서 비활성화됩니다.

> **참고:** 규칙에 여러 정책 값이 지정된 경우(예: policy security-ips drop, policy balanced-ips drop), 두 정책 모두에 나타납니다. 지정된 규칙에 대해 지정된 정책 값이 없는 경우 기본적으로 정책 없이 표시됩니다.

관리되는 디바이스가 패시브 모드로 설정되고 정책이 삭제되도록 설정된 경우 이 작업은 아무런 효과가 없습니다. 디바이스에서 알림을 생성합니다. 디바이스가 인라인 모드에 있고 정책 값이

drop으로 설정된 경우 규칙은 기본적으로 패킷을 삭제합니다. 정책 값이 alert로 설정된 경우 삭제 없이 이벤트만 생성합니다.

마지막으로, 대부분의 경우 패킷이 삭제되면 알림이 생성됩니다. 지정된 규칙에 대해 경고의 억제가 독립적으로 구성되지 않는 한 이는 마찬가지입니다.

Sourcefire는 새 규칙에 대해 적절한 기본 상태를 어떻게 결정합니까?

규칙의 기본 상태는 여러 요소를 기반으로 합니다. 예를 들면 다음과 같습니다.

영향

고려해야 할 사항

이러한 취약성을 악용하려는 시도가 얼마나 일어날 가능성이 있으며, Cisco 사용자(Sourcefire 고객 및 더 광범위한 Snort 커뮤니티 모두)의 몇 퍼센트가 이러한 취약성에 취약해질 것으로 예상됩니까?

기억해야 할 사항

야생에서 알려진 공격이 있는 Internet Explorer 취약성은 권한이 잘못 구성되었을 때 악의적으로 사용할 수 있는 SAP 데이터베이스 기능이나 Linux 커널의 알려지지 않은 모듈에서 복잡한 서비스 거부 공격보다 훨씬 더 큰 영향을 미칩니다. VRT는 취약성의 CVSS 점수로 시작하여, 우리가 보유하고 있는 추가 정보로 필요에 따라 조정합니다. 이 메트릭은 가장 중요한 메트릭입니다. 영향을 충분히 높이면 규칙을 활성화하지 않거나 삭제하도록 설정하지 않기 때문입니다.

성능

고려해야 할 사항

"평균" 네트워크에서 이 규칙이 빠르고 느리다고 예상합니까?

기억해야 할 사항

규칙의 속도는 검사 중인 트래픽에 전적으로 의존하여 성능을 측정하기 어려운 반면, 일반 네트워크를 구성하는 것과 해당 규칙이 일반 네트워크에서 수행하는 방식에 대한 일반적인 이해가 있습니다. 예를 들어 비교적 긴(6바이트 이상, 일반적으로) 비교적 고유한 단일 콘텐츠 일치(예: "unbigestJavaScriptFunction()", "|00 00 00|" 또는 "GET / HTTP/1.1")은 복잡한 PCRE, 일련의 byte_test 및/또는 byte_jump 절을 가진 규칙보다 빠르게 평가됩니다. 이러한 정보를 통해 규칙이 빠르고 느리는지를 확인하고 이를 고려할 수 있습니다.

신뢰도

고려해야 할 사항

이 규칙이 오탐을 생성할 가능성은 얼마나 됩니까?

기억해야 할 사항

일부 취약점은 공격을 받기 위해 매우 구체적이고 쉽게 탐지된 조건이 있어야 하며, 이 경우 관련 규칙이 발생할 때마다 라이브 익스플로잇이 진행 중임을 매우 확신할 수 있습니다. 예를 들어, 고정된 위치에 고유한 매직 문자열이 있는 프로토콜에 버퍼 오버플로가 있고 그 매직 문자열에서 고정된 거리인 지정된 길이가 있으면 매직 문자열을 찾아서 알려진 문제 값을 기준으로 확인할 수 있습니다. 다른 경우에는 문제가 훨씬 덜 잘 정의되어 있습니다. 예를 들어 특정 DNS 캐시 중독 공격은 특정 기간 동안 서버에서 비정상적으로 많은 수의 NXDOMAIN 회신으로 나타날 수 있습니다. 이러한 경우 NXDOMAIN 회신의 단순한 존재 자체가 익스플로잇을 나타내는 것이 아닙니다. 문제를 나타내는 짧은 시간에 매우 많은 수의 회신이 있는 것입니다. 이 수는 다른 네트워크에 대해 다르기 때문에 VRT는 대부분의 네트워크에서 사용할 값을 선택하고 이를 릴리스해야 합니다. 그러나 규칙이 발생할 때 실제 악의적인 활동이 발생한다고 100% 확신할 수는 없습니다.

적어도 중요한 것은, 때때로 다른 요인을 고려하는 것은 사실이지만, 결국 결국에는 피해를 초래할 수 있다는 점입니다. 즉, 고객이 야생에서 가장 많이 볼 수 있는 위협으로부터 고객을 보호할 수 있도록 하는 것이 Cisco의 주요 관심사입니다.