문서등급	공개

IPv6 취약점 탐지 기술

목 차

1. 개요 3
2. 룰의 형식 4
3. 호환성 5
3.1 룰의 프로토콜 명시 5
3.2 상위 프로토콜 탐지 5
4. 탐지 옵션 6
4.1 IPv6 헤더 탐지 옵션 6
4.1.1 ip6_tc 6
4.1.2 ip6_fl 6
4.1.3 ip6_nh 6
4.1.4 Hop Limit 7
4.2 확장 헤더 탐지 옵션 8
4.2.1 ip6_otype 8
4.2.2 ip6_id 8
4.2.3 ip6_fragoffset 8
4.2.4 ip6_fragbits 9
4.3 ICMPv6 탐지 옵션 10
4.3.1 icmp6_type 10
4.3.2 icmp6_code 10
4.3.3 icmp6_id 10
4.3.4 icmp6_seq 10
4.3.5 icmp6_otype 11
4.3.6 icmp6_olen 11
4.3.7 icmp6_rl 11
4.3.8 icmp6_vl 12
4.3.9 icmp6_pl 12
용어 정리 14
연락처 14
회사 소개 14

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

표 목 차

<표 1> IPv6 헤더 탐지 옵션 및 설명 7
<표 2> 확장 헤더 탐지 옵션 및 설명 9
<표 3> ICMPv6 탐지 옵션 및 설명 12

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

1. 개요

본 문서는 IPv6 취약점을 탐지하기 위한 탐지 룰 및 탐지 옵션에 대한 기술을 다룬다. 기존 Snort 와 같은 룰 기반의 IDS/IPS 에서 적용 가능 한 형태의 탐지 옵션을 의미한다. IPv6 헤더, 확장헤더, ICMPv6 를 검사하기 위한 전용 탐지 옵션을 정의하며 기존 룰과의 호환성에 대한 내용을 서술한다.

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

2. 룰의 형식

기존 snort 룰의 형식과 IPv6 취약점을 탐지하기 위한 룰의 형식은 다음과 같다. 기존 snort 룰과 동일하게 사용된다. 룰 옵션에는 IPv6 헤더와 관련된 필드를 탐지하기 위한 옵션들이 사용될 수 있다.

- Snort (TCP) : alert tcp any any -> any any (content:"test";)
- Snort (IP) : alert ip any any -> any any (ttl:3;)
- Snort (ICMP) : alert icmp any any -> any any (itype:8;)
- IPv6 취약점 탐지 룰 : alert ip any any -> any any (ip6_nh:fragment; icmp6_type:134; icmp6_otype:3; icmp6_olen:>4;)

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

3. 호환성

3.1 룰의 프로토콜 명시

IPv6 및 ICMPv6는 기존 룰이 사용하는 프로토콜인 IP, TCP, UDP, ICMP 내에 포함된다. 즉, IPv6 취약점을 탐지하기 위해서 룰 내의 protocol 필드 부분에 "ipv6" 형식으로 넣지 않아도 된다. 아래 룰들은 이해를 돕기 위한 예제이다.

- alert ip any any -> any any (ttl:6;)
  IPv4 의 TTL 필드가 6 인지 검사한다.
- alert ipv6 any any -> any any (ip6_nh:6;)
  잘못된 예제이다.
- alert ip any any -> any any (ip6_nh:6;)
  IPv6 의 Next Hop 필드가 6 인지 검사한다.
- alert icmp any any -> any any (icmp6_type:134; icmp6_otype:3; icmp6_vl:infinity; icmp6_pl:infinity;)
  ICMPv6 의 타입으로 134 (Router Advertisement), option 타입으로 3 (prefix information), valid lifetime, preferred lifetime 이 각각 무한대인 경우를 검사한다.

3.2 상위 프로토콜 탐지

탐지 룰이 TCP 혹은 UDP일 경우 룰은 IPv4 혹은 IPv6 환경에서 동일하게 적용되며 탐지된다.

- alert tcp any any -> any any (content:"test";)
  IPv4 환경 혹은 IPv6 환경에서의 TCP 프로토콜 내의 데이터 페이로드에서 test라는 문자열을 찾는다.

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

4. 탐지 옵션

옵션 종류는 IPv6 헤더, 확장 헤더, ICMPv6 로 분류할 수 있다.

4.1 IPv6 헤더 탐지 옵션

IPv6 헤더 탐지 옵션의 종류는 다음과 같다.

4.1.1 ip6_tc

ip6_tc는 IPv6 헤더의 Traffic Class 필드를 검사한다. Traffic Class는 IPv6 패킷의 클래스나 우선순위를 나타낸다. IPv4 의 TOS와 동일한 기능을 수행한다.

- 사용법
  - ✓ ip6_tc:[!]<number>;

- 예제
  - ✓ ip6_tc:!4;

4.1.2 ip6_fl

ip6_fl은 IPv6 헤더의 Flow Label 필드를 검사한다. Flow Label는 라우터의 실시간 처리, QoS 처리 등 특별한 처리를 요구한다. Flow label 지원하지 않는 호스트/라우터는 패킷 생성시 0으로 설정한다.

- 사용법
  - ✓ ip6_fl:[!|<|>]<number>;

- 예제
  - ✓ ip6_fl:1000;

4.1.3 ip6_nh

ip6_nh는 IPv6 헤더의 Next Header 필드를 검사한다. Next Header는 IPv6 헤더 뒤에 오는 헤더의 타입을 명시한다.

- 사용법
  - ✓ ip6_nh:[!|<|>]<name or number>;

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

- 예제
  - ✓ ip6_nh:6;
  - ✓ ip6_nh:tcp;

4.1.4 Hop Limit

ip6_hl은 IPv6 헤더의 Hop Limit 필드를 검사한다. Hop Limit는 각 노드를 지날 때 1씩 감소한다. 0일 경우 패킷을 버린다. IPv4의 TTL 필드와 동일한 역할을 수행한다.

- 사용법
  - ✓ ip6_hl:[<, >, =, <=, >=]<number>;
  - ✓ ip6_hl:[<number>]-[<number>];

- 예제
  - ✓ ip6_hl:<3;
  - ✓ ip6_hl:3-5; (3~5)
  - ✓ ip6_hl:-5; (0~5)
  - ✓ ip6_hl:5-; (5~255)
  - ✓ ip6_hl:<=5;
  - ✓ ip6_hl:>=5;
  - ✓ ip6_hl:=5;

<표 1> IPv6 헤더 탐지 옵션 및 설명

순번	필드 명	탐지옵션 명	탐지 옵션 설명
1	Traffic Class	ip6_tc	ip6_tc는 IPv6 헤더의 Traffic Class 필드를 검사한다.
2	Flow Label	ip6_fl	ip6_fl은 IPv6 헤더의 Flow Label 필드를 검사한다.
3	Next Header	ip6_nh	ip6_nh는 IPv6 헤더의 Next Header 필드를 검사한다.
4	Hop Limit	ip6_hl	ip6_hl은 IPv6 헤더의 Hop Limit 필드를 검사한다.

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

4.2 확장 헤더 탐지 옵션

확장 헤더는 IPv6 헤더의 Next Header 필드의 값으로 구별할 수 있다. IPv6 확장 헤더 탐지 옵션의 종류는 다음과 같다.

4.2.1 ip6_otype

ip6_otype은 확장 헤더 중 Hop-By-Hop Options 헤더와 Destination Options 헤더 내에 존재하는 옵션 타입 필드를 검사한다.

- 사용법
  - ✓ ip6_otype:min<>max;
  - ✓ ip6_otype:[<|>]<number>;

- 예제
  - ✓ ip6_otype:128;

4.2.2 ip6_id

ip6_id는 확장 헤더 중 Fragment 헤더 내의 Identification 필드를 검사한다. IPv4 헤더의 Identification 과 동일한 역할을 수행한다. IPv4는 16bit, IPv6는 32bit이다.

- 사용법
  - ✓ ip6_id:<number>;

- 예제
  - ✓ ip6_id:31337;

4.2.3 ip6_fragoffset

ip6_fragoffset은 확장 헤더 중 Fragment 헤더 내의 Fragoffset 필드를 검사한다. IPv4 헤더의 Fragoffset 과 동일한 역할을 수행한다.

- 사용법
  - ✓ ip6_fragoffset:[!|<|>]<number>;

- 예제
  - ✓ ip6_fragoffset:0;

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

4.2.4 ip6_fragbits

ip6_fragbits는 확장 헤더 중 Fragment 헤더 내의 Fragbits 필드를 검사한다. IPv4 헤더의 Fragbits와 동일한 역할을 수행한다. IPv6의 M플래그는 1혹은 0이며 Reserved 비트는 2비트로 사용하지 않으므로 0으로 설정되어 있다.

- 사용법
  - ✓ ip6_fragbits:<[MD]>;

- 예제
  - ✓ ip6_fragbits:M;

<표 2> 확장 헤더 탐지 옵션 및 설명

순번	필드 명	탐지옵션 명	탐지 옵션 설명
1	option type	ip6_otype	ip6_otype은 확장 헤더 중 Hop-By-Hop Options 헤더와 Destination Options 헤더 내에 존재하는 옵션 타입 필드를 검사한다.
2	EXTENSION HEADER fragment id	ip6_id	ip6_id는 확장 헤더 중 Fragment 헤더 내의 Identification 필드를 검사한다.
3	EXTENSION HEADER fragment offset	ip6_fragoffset	ip6_fragoffset은 확장 헤더 중 Fragment 헤더 내의 Fragoffset 필드를 검사한다.
4	EXTENSION HEADER fragment bits	ip6_fragbits	ip6_fragbits는 확장 헤더 중 Fragment 헤더 내의 Fragbits 필드를 검사한다.

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

4.3 ICMPv6 탐지 옵션

ICMPv6 탐지 옵션은 다음과 같다.

4.3.1 icmp6_type

icmp6_type은 ICMPv6의 Type 필드를 검사한다.

- 사용법
  - ✓ icmp6_type:min<>max;
  - ✓ icmp6_type:[<|>]<number>;

- 예제
  - ✓ icmp6_type:>30;

4.3.2 icmp6_code

icmp6_code은 ICMPv6의 Code 필드를 검사한다.

- 사용법
  - ✓ icmp6_code:min<>max;
  - ✓ icmp6_code:[<|>]<number>;

- 예제
  - ✓ icmp6_code:>30;

4.3.3 icmp6_id

icmp6_id는 ICMPv6의 Echo Request Message의 Identification 필드를 검사한다.

- 사용법
  - ✓ icmp6_id:<number>;

- 예제
  - ✓ icmp6_id:0;

4.3.4 icmp6_seq

icmp6_seq는 ICMPv6의 Echo Request Message의 Sequence Number 필드를 검사한다.

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

- 사용법
  - ✓ icmp6_seq:<number>;

- 예제
  - ✓ icmp6_seq:0;

4.3.5 icmp6_otype

icmp6_otype은 ICMPv6의 Neighbor Discovery의 각 Option의 타입 필드를 검사한다.

- 사용법
  - ✓ icmp6_otype:<name or number>;

- 이름정의
  - ✓ sla – Source Link-Layer Address
  - ✓ tla – Target Link-Layer Address
  - ✓ pi – Prefix Information
  - ✓ rh – Redirected Header
  - ✓ MTU – MTU

- 예제
  - ✓ icmp6_otype:3;
  - ✓ icmp6_otype:pi

4.3.6 icmp6_olen

icmp6_olen은 ICMPv6의 Neighbor Discovery의 각 Option의 길이 필드를 검사한다.

- 사용법
  - ✓ icmp6_olen:[<, >, =, <=, >=]<number>;

- 예제
  - ✓ icmp6_olen:4;

4.3.7 icmp6_rl

icmp6_rl은 ICMPv6의 Neighbor Discovery Router Advertisement의 Router lifetime 필드를 검사한다.

- 사용법

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

- ✓ icmp6_rl:[<, >, =, <=, >=]<number>;

■ 예제

- ✓ icmp6_rl:0;

4.3.8 icmp6_vl

icmp6_vl은 ICMPv6의 Neighbor Discovery Router Advertisement의 valid lifetime 필드를 검사한다.

■ 사용법

- ✓ icmp6_vl:[<, >, =, <=, >=]<number or name>;

■ 예제

- ✓ icmp6_vl:100000;
- ✓ icmp6_vl:infinity; (32bit all 1)

4.3.9 icmp6_pl

icmp6_pl은 ICMPv6의 Neighbor Discovery Router Advertisement의 preferred lifetime 필드를 검사한다.

■ 사용법

- ✓ icmp6_pl:[<, >, =, <=, >=]<number or name>;

■ 예제

- ✓ icmp6_pl:100000;
- ✓ icmp6_pl:infinity; (32bit all 1)

<표 3> ICMPv6 탐지 옵션 및 설명

순번	필드 명	탐지옵션 명	탐지 옵션 설명
1	ICMPv6 type	icmp6_type	icmp6_type은 ICMPv6의 Type 필드를 검사한다.
2	ICMPv6 code	icmp6_code	icmp6_code은 ICMPv6의 Code 필드를 검사한다.
3	ICMPv6 echo id	icmp6_id	icmp6_id는 ICMPv6의 Echo Request Message의 Identification 필드를 검사한다.
4	ICMPv6 echo seq	icmp6_seq	icmp6_seq는 ICMPv6의 Echo Request Message의 Sequence Number 필드를 검사한다.
5	ICMPv6 option type	icmp6_otype	icmp6_otype은 ICMPv6의 Neighbor Discovery의 각 Option의 타입 필드를 검사한다.

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

6	ICMPv6 option length	icmp6_olen	icmp6_olen은 ICMPv6의 Neighbor Discovery의 각 Option의 길이 필드를 검사한다.
7	ICMPv6 ND Router lifetime	icmp6_rl	icmp6_rl은 ICMPv6의 Neighbor Discovery Router Advertisement의 Router lifetime 필드를 검사한다.
8	ICMPv6 ND valid lifetime	icmp6_vl	icmp6_vl은 ICMPv6의 Neighbor Discovery Router Advertisement의 valid lifetime 필드를 검사한다.
9	ICMPv6 ND preferred lifetime	icmp6_pl	icmp6_pl은 ICMPv6의 Neighbor Discovery Router Advertisement의 preferred lifetime 필드를 검사한다.

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –

용어 정리

본 보고서에서 사용된 용어들에 대한 정리는 아래 glossary를 참조하십시오.
https://tms.infosec.co.kr/SClient2/community/word.php?c2=C0006

연락처

문서와 관련된 궁금 사항 발생 시 아래 연락처로 연락하시기 바랍니다.

E-mail	cert@infosec.co.kr
전화	02-6003-0953
FAX접수	02-3445-0991

회사 소개

㈜정보보호기술은 침입탐지시스템(TESS IDS) 연구/개발 분야에서, K4 인증, OPSEC 인증, ICSA 인증, NOKIA 인증 및 CHECKMARK 인증 등 전세계 공인 인증 기관 및 산업 표준 인증 획득을 통하여 기술력과 우수성을 인정 받았습니다. 이러한 기술을 바탕으로, 위협분석시스템(TESS TAS) 및 위협관리시스템(TESS TMS) 등으로 솔루션 개발 분야를 확대하고, 글로벌 조기 예/경보 서비스 및 긴급 취약성 경보 서비스를 제공하는 위협관리 전문기업입니다.

최근 인터넷 웜, 바이러스, 해킹 등의 사이버 위협에 대한 종합적인 대응 체계로서, 주요 정부 기관 및 ISP들이 연이어 ㈜정보보호기술의 위협관리 솔루션 및 서비스를 채택함으로써 ㈜정보보호기술의 위협관리 전문기업으로서의 위상을 확고히 하고 있습니다.

어떠한 보안 제품도 "Magic Security"를 만족할 수 없습니다. 활성화된 위협의 형태, 원인 및 현상에 따라 적절한 보안 수단을 적용할 수 있도록 Technology(솔루션)과 Information(서비스)가 상호 유기적으로 결합되어야만 합니다.

㈜정보보호기술은 사이버 위협으로부터 고객의 소중한 자산을 안전하게 보호할 수 있도록 종합적인 솔루션 및 서비스를 제공하도록 언제나 최선을 다하여 노력하겠습니다.

회 사 명 : ㈜정보보호기술 (INFOSEC Technologies Co., Ltd.) http://www.infosec.co.kr/

- 대표이사 : 조명제
- 설립일자 : 2000년 4월 7일
- 소재지 : 서울시 강남구 논현동 57-38번지 원영빌딩 3층~5층 (우:135-010)
- 대표전화 : 02-6003-0999 FAX : 02-3445-0991
- 사업영역 : 위협관리솔루션 및 서비스 판매

– Copyright ⓒ 2012 ㈜정보보호기술. All rights reserved. –