한국인터넷진흥원

DNS 신규취약점 조치 권고

2024. 2. 29. (목), 한국인터넷정보센터

□ 개요

o DNS 신규 취약점(DNS Key Trap, CVE-2023-50387) 공개(2.14.)에 따른 DNS 운영현황 점검 및 취약점 조치 권고

※ 보안뉴스, 2024.2.19. "인터넷 일부 마비시킬 수 있는 DNS 취약점 키트랩 공개돼"

□ 취약점 주요내용

o (대상) **DNSSEC 기능을 사용하는 캐시DNS**

o (내용) DNS 보안기능(DNSSEC)의 서명검증 중 과도한 연산처리를 유발하여 캐시DNS 서버의 CPU 자원을 소모시키는 취약점으로 **특정 DNS S/W의 취약점이 아닌 DNSSEC 표준 프로토콜의 취약점**

o (취약점 동작원리) 서명검증에 필요한 레코드가 다수인 경우, **캐시DNS가 모든 경우에 대해 서명검증을 수행**하는 DNSSEC 프로토콜을 악용

- 현재 DNSSEC 표준은 서명검증 기능이 활성화 된 캐시DNS 서버가 DNSSEC이 서명된 DNS 레코드를 응답받았을 때, 서명데이터(RRSIG) 검증이 올바른 경우가 발견될 때까지 지정된 서명알고리즘별 서명키의 공개키(DNSKEY)를 조회하여 서명검증 수행

- 예를들어, 서비스 중단없는 DNSSEC 서명키 교체를 위해 캐시DNS의 TTL 등의 요소를 고려하여 DNSKEY 레코드를 2개 이상 설정하고 있으며, DNSSEC 프로토콜에서는 DNS 서비스 안정성 보장을 위해 모든 DNSKEY 레코드를 조회하여 검증 수행

- 공격자는 이를 악용하여 자신의 도메인에 데이터를 조작한 **서명레코드(RRSIG) 및 공개키 레코드(DNSKEY)를 과도한 개수로 설정** 후, 공격 대상 캐시DNS에 자신의 도메인에 DNS 질의하여 KeyTrap 공격 가능

※ 현재 DNSSEC 표준은 DNS 레코드에 대해 설정할 수 있는 **서명레코드(RRSIG) 및 도메인의 공개키(DNSKEY) 개수 제한 없음**

o BIND의 경우 S/W 패치버전 적용으로 일부 완화되었지만, KeyTrap 취약점 악용한 대규모 DNS질의를 사용하는 공격시도가 있는 경우, 공격 질의 트래픽에 비례하여 서버시스템의 CPU 부하 유발 가능

- 캐시DNS 서버에서 DNSSEC 검증 시, CPU를 최대 50%만 소비하도록 제한하여 공격으로 인한 CPU 과부하 방지 및 DNS 서비스 복원력 향상

- 공격용 도메인은 .kr, .com, .net 등 전체 도메인이 대상이므로, 공격사전 점검은 현실적으로 어려우며, **시스템 리소스 및 서비스 집중 모니터링 필요**

□ 권고사항

o 이용 중인 **DNS S/W별 신속한 패치버전 업그레이드** 권고

S/W	최신버전
Microsoft DNS	2024년 2월 13일 이후 출시 버전
BIND9	9.16.46, 9.18.22, 9.19.20 이상 버전
PowerDNS Recursor	4.8.6, 4.9.3, 5.0.2 이상 버전
unbound	1.19.1 버전
Knot Resolver	5.7.1 버전

o 의도적으로 오픈DNS 서비스를 제공하는 등의 특별한 사유가 없는 경우, **외부 사용자의 캐시DNS 질의 차단 설정** 권고

※ BIND의 경우, "allow-recursion" 옵션 사용하여 DNS 질의응답 처리 제공 대상 "질의호스트 제한" 설정 가능

□ 문의사항

o 한국인터넷진흥원 인터넷주소기술팀 (061-820-2858, in_chk@nic.or.kr)

□ 참고정보

[1] ISC, "CVE-2023-50387: KeyTrap - Extreme CPU consumption in DNSSEC validator"
- https://kb.isc.org/v1/docs/cve-2023-50387

[2] PowerDNS, "PowerDNS Recursor Security Advisory 2024-01"
- https://blog.powerdns.com/2024/02/13/powerdns-recursor-4-8-6-4-9-3-5-0-2-released

[3] CZ.NIC, "Knot Resolver 5.7.1 (2024-02-13)"
- https://gitlab.nic.cz/knot/knot-resolver/-/releases/v5.7.1

[4] ISC, "BIND 9 Security Release and Multi-Vendor Vulnerability Handling, CVE-2023-50387 and CVE-2023-50868"
- https://www.isc.org/blogs/2024-bind-security-release/

[5] APNIC, "KeyTrap algorithmic complexity attacks exploit fundamental design flaw in DNSSEC"
- https://blog.apnic.net/2024/02/19/keytrap-algorithmic-complexity-attacks-exploit-fundamental-design-flaw-in-dnssec/

붙임1 DNSSEC 활성화 여부 점검 방안

o DNSSEC 서명검증 테스트용 질의를 통해 DNSSEC 활성화 여부 점검

- (질의 명령어) dig dnssec-failed.org +dnssec +nocrypto @<캐시DNS_IP>

※ (활성화 상태) 응답 데이터 없이 SERVFAIL 에러코드로 응답

※ (비활성화 상태) ANSWER SECTION에 A 및 RRSIG 레코드 설정 응답

서명검증 **활성화** 상태 경우, 질의 및 응답**(파란색)** 예시

```
$ dig dnssec-failed.org +dnssec +nocrypto @캐시DNS IP

; <<>> DiG 9.18.19 <<>> dnssec-failed.org +dnssec +nocrypto @xxx.xxx.xxx.xxx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 59051
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
; EDE: 9 (DNSKEY Missing): (No DNSKEY matches DS RRs of dnssec-failed.org)
;; QUESTION SECTION:
;dnssec-failed.org.              IN      A

;; Query time: 387 msec
;; SERVER: xxx.xxx.xxx.xxx#53(xxx.xxx.xxx.xxx) (UDP)
;; WHEN: Thu Feb 22 16:18:48 KST 2024
;; MSG SIZE  rcvd: 97

$
```

서명검증 **비활성화** 상태 경우, 질의 및 응답**(빨간색)** 예시

```
$ dig dnssec-failed.org +dnssec +nocrypto @캐시DNS IP

; <<>> DiG 9.18.19 <<>> dnssec-failed.org +dnssec @xxx.xxx.xxx.xxx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56121
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: 18d8ebb0347997970100000065d6f418733c9520620da37b (good)
;; QUESTION SECTION:
;dnssec-failed.org.              IN      A

;; ANSWER SECTION:
dnssec-failed.org.      300     IN      A       96.99.227.255
dnssec-failed.org.      300     IN      RRSIG   A 5 2 300 20240306145112 20240218144612 44973
dnssec-failed.org. [omitted]

;; Query time: 197 msec
;; SERVER: xxx.xxx.xxx.xxx#53(xxx.xxx.xxx.xxx) (UDP)
;; WHEN: Thu Feb 22 16:13:28 KST 2024
;; MSG SIZE  rcvd: 267

$
```

붙임2 질의호스트 제한 설정

o BIND 질의호스트 제한 설정 방안

- BIND 설정파일(named.conf)에 인가된 호스트(내부사용자)만 캐시DNS를 이용할 수 있도록 ACL 설정 권고

```
acl "ourhosts" {          // [ACL 정의] ACL 이름(ourhosts)은 운영자가 적절한 이름으로 설정하여 사용
  localhost;
  localnets;
  xxx.xxx.xxx.xxx/16;    // 질의 허용할 호스트의 IP Prefix 설정
  xxx.xxx.xxx.xxx/24;    //
  ...
};

options {
  ...
  recursion yes;                    // 캐시DNS 서버 동작여부 설정
  allow-recursion { ourhosts; };  // ACL "ourhosts"에 지정된 호스트의 질의만 허용
  ...
};
```