NTTデータ・セキュリティ株式会社

BIND の Dynamic Update 機能の脆弱性（CVE-2009-0696）に関する検証レポート

2009/8/3
2009/8/4(更新)
診断ビジネス部
辻 伸弘
松田 和之

【概要】

ISC の BIND の Dynamic Update 機能に脆弱性が存在することが発見されました。
この脆弱性により、細工された Dynamic Update パケットを送信された場合に、DNS サービスを停止される恐れがあります。
Dynamic Update 機能とは、クライアントから DNS サーバが管理するゾーン情報の動的更新を可能にする機能です。
本脆弱性は、Dynamic Update 機能を有効にしていないシステムでも影響を受けます。

今回、BIND の Dynamic Update 機能の脆弱性（CVE-2009-0696）の再現性について検証を行いました。

【影響を受けるとされているシステム】

BIND 9 すべてのバージョン

【対策案】

ISC から、修正プログラムがリリースされています。
充分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラムの適用を行うことが推奨されます。

BIND 9.6.1-P1
http://ftp.isc.org/isc/bind9/9.6.1-P1/bind-9.6.1-P1.tar.gz
BIND 9.5.1-P3
http://ftp.isc.org/isc/bind9/9.5.1-P3/bind-9.5.1-P3.tar.gz
BIND 9.4.3-P3
http://ftp.isc.org/isc/bind9/9.4.3-P3/bind-9.4.3-P3.tar.gz

なお、9.3 以前のバージョンは、サポートが終了しているため修正プログラムがリリースされません。
そのため、9.4 以降の最新のバージョンにアップデートすることが推奨されます。

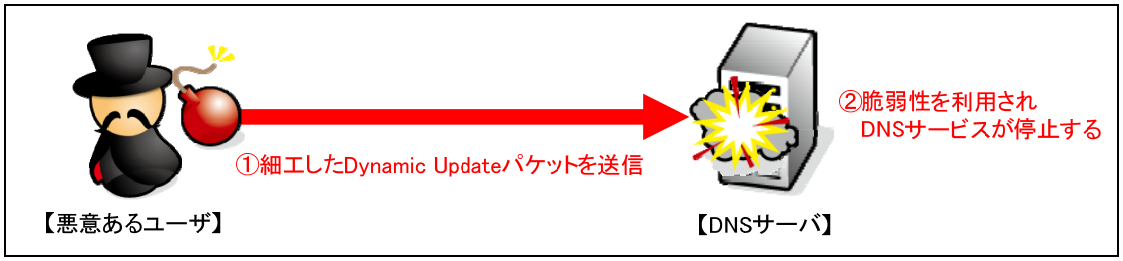
【参考サイト】

BIND Dynamic Update DoS | Internet Systems Consortium
https://www.isc.org/node/474

CVE-2009-0696
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0696

NTTデータ・セキュリティ株式会社

【検証イメージ】



【検証ターゲットシステム】

CentOS 4.4
BIND 9.4.0

【検証概要】

ターゲットシステムに、細工した Dynamic Update パケットを送信することでサービス停止させます。

【検証結果】

下図の赤線で囲まれている部分は、細工した Dynamic Update パケットを送信する前の名前解決の問合せ結果を示しています。問合せに対して、正常に応答していることが確認できます。
黄線で囲まれている部分は、細工した Dynamic Update パケット送信後のターゲットシステムに対して、名前解決の問合せをした結果を示しています。DNS サーバに接続できずタイムアウトとなっていることが確認できます。
これにより、ターゲットシステムの DNS サービスの停止に成功したと言えます。

ターゲットシステムの DNS サービスの停止に成功した画面

```
[root@localhost pen-test]# dig @10.100.0.130 dns.nttdata-sec.co.jp

; <<>> DiG 9.2.4 <<>> @10.100.0.130 dns.nttdata-sec.co.jp
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65353
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;dns.nttdata-sec.co.jp.         IN      A

;; ANSWER SECTION:
dns.nttdata-sec.co.jp.  86400   IN      A       10.100.0.106

;; AUTHORITY SECTION:
nttdata-sec.co.jp.      86400   IN      NS      dns.nttdata-sec.co.jp.

;; Query time: 23 msec
;; SERVER: 10.100.0.130#53(10.100.0.130)
;; WHEN: Mon Aug  3 11:07:54 2009
;; MSG SIZE  rcvd: 69

[root@localhost pen-test]#
[root@localhost pen-test]#
[root@localhost pen-test]# ./bind9_dos 10.100.0.130 nttdata-sec.co.jp
done
[root@localhost pen-test]#
[root@localhost pen-test]#
[root@localhost pen-test]# dig @10.100.0.130 dns.nttdata-sec.co.jp

; <<>> DiG 9.2.4 <<>> @10.100.0.130 dns.nttdata-sec.co.jp
; (1 server found)
;; global options:  printcmd
;; connection timed out; no servers could be reached
[root@localhost pen-test]#
```

下図の赤線で囲まれている部分は、細工した Dynamic Update パケットを送信する前のターゲットシステム上のプロセス確認結果を示しています。BIND のプロセスである named が稼動していることが確認できます。
黄線で囲まれている部分は、細工した Dynamic Update パケット送信した後のプロセス確認結果を示しています。BIND のプロセス named が存在しないことが確認できます。
これにより、ターゲットシステムの DNS サービスの停止に成功したと言えます。

ターゲットシステムの DNS サービスのプロセス

```
[root@victim ~]# ps -A | grep named
 4618 ?        00:00:00 named
[root@victim ~]#
[root@victim ~]# ps -A | grep named
[root@victim ~]#
```

下図の赤線で囲まれている部分は、細工した Dynamic Update パケットを送信した後の BIND のログを示しています。
これにより、BIND でエラーが発生し、サービスの停止に成功したと判断できます。

ターゲットシステムの DNS サービスのログ

```
Aug  3 11:32:03 victim named[4598]: starting BIND 9.2.4 -u named
Aug  3 11:32:03 victim named[4598]: using 1 CPU
Aug  3 11:32:03 victim named[4598]: loading configuration from '/etc/named.conf'
Aug  3 11:32:03 victim named[4598]: listening on IPv4 interface lo, 127.0.0.1#53
Aug  3 11:32:03 victim named[4598]: listening on IPv4 interface eth0, 10.100.0.130#53
Aug  3 11:32:03 victim named[4598]: command channel listening on 127.0.0.1#953
Aug  3 11:32:03 victim named[4598]: command channel listening on ::1#953
Aug  3 11:32:03 victim named[4598]: zone nttdata-sec.co.jp/IN: loaded serial 2002122001
Aug  3 11:32:03 victim named: named 起動 succeeded
Aug  3 11:32:03 victim named[4598]: running
Aug  3 11:32:14 victim named[4598]: db.c:579: REQUIRE(type != ((dns_rdatatype_t)dns_rdatat
ype_any)) failed
Aug  3 11:32:14 victim named[4598]: exiting (due to assertion failure)
```

【対策案】

ISC から、修正プログラムがリリースされています。
充分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラムの適用を行うことが推奨されます。

BIND 9.6.1-P1
http://ftp.isc.org/isc/bind9/9.6.1-P1/bind-9.6.1-P1.tar.gz
BIND 9.5.1-P3
http://ftp.isc.org/isc/bind9/9.5.1-P3/bind-9.5.1-P3.tar.gz
BIND 9.4.3-P3
http://ftp.isc.org/isc/bind9/9.4.3-P3/bind-9.4.3-P3.tar.gz

なお、9.3 以前のバージョンは、サポートが終了しているため修正プログラムがリリースされません。
そのため、9.4 以降の最新のバージョンにアップデートすることが推奨されます。

【参考サイト】

BIND Dynamic Update DoS | Internet Systems Consortium
https://www.isc.org/node/474

CVE-2009-0696
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0696

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】

NTT データ･セキュリティ株式会社

NTTデータ・セキュリティ株式会社

営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/