リリース 5 以前の RedHat Enterprise Linux およびその互換 OS をセカンダリサーバとして用いるゾーンへの DNSSEC の導入にあたっての注意喚起

平成 23 年 10 月

DNSSEC ジャパン 運用技術 WG

はじめに

この文書では、リリース 5 以前の RedHat Enterprise Linux およびその互換 OS をセカンダリサーバとして用いているゾーンで DNSSEC を有効にしたときに観測された問題点を示し、DNS の運用者に、当該事象に対する注意を喚起したい。

ここで示す問題は、セカンダリサーバの運用者が DNSSEC への対応を意図していない場合に起きることに注意されたい。

問題の要点は
- セカンダリサーバの運用者が関知しないところでプライマリサーバの運用者のみによって引き起こされ得る。
- サーバホストの OS として広く用いられている RedHat Enterprise Linux およびその互換 OS の 5 以前のリリースで発生し得る。
- セカンダリサーバの管理者がセキュリティホールへの対応を心がけ、RPM パッケージのアップデートに迅速に追従していても、発生し得る。
の 3 点に集約される。

なお、本質的には上で述べた OS に固有の問題ではなく、古いバージョンの BIND(9.3 以前、あるいは 9.5 以前)を用いる場合の問題である。ただし、いずれのバージョンも、RedHat Enterprise Linux およびその互換 OS では、OS のリリース元が独自のメンテナンスによりサポートを継続しており、BIND のリリース元である ISC では、既に End of Life の扱いとなっている。

想定している状況

ここでは
- セカンダリサーバの運用者が、DNSSEC への対応を意図していない。

- セカンダリサーバのバージョンが古い。この文書では 2 つの問題点を指摘するが、うち 1 つは 9.3 以前、もう 1 つは 9.5 以前のバージョンを用いているときに発生する。
- プライマリサーバの運用者が DNSSEC を有効にした。すなわち、プライマリサーバが署名したゾーンデータを提供するとともに、レジストラへ所定の手続きをとるなどの方法により、上位ゾーンに DS RR を登録した。

という状況を想定して議論する。

観測された問題 その 1

DNSSEC の validation を有効にしているキャッシュサーバが、再帰的問い合わせの過程でセカンダリサーバから応答を得ると、validation に失敗する。

BIND 9.3 では、named.conf の options {}ステートメントにおける設定パラメータ dnssec-enable のデフォルト値は no である。想定している状況から、明示的に yes とは設定されてないものとすると、上位ゾーンには当該ゾーンの DS RR が含まれているにも関わらず、セカンダリサーバは当該ゾーンに関する DNSKEY RR を提供しないので、validation に失敗する。また、BIND 9.2 以前は、現在のインターネットで用いられている RFC 4033～4035 に基づく DNSSEC をサポートしていないので、同様の問題が起こる。

なお、dnssec-enable のデフォルト値は BIND 9.4 から yes に変更されているので、BIND 9.4 以降では明示的に yes と設定しなくても、この問題は発生しない。ただし、DNSSEC を有効にしないという明確な意思の下、明示的に no と設定していると、同じ問題が発生する。

この問題が発生した際には、スタブレゾルバは正当な名前の解決に失敗するので、影響は大きい。

観測された問題 その 2

当該ゾーンが不在証明の方式として NSEC3 を採用しているとき、DNSSEC の validation を有効にしているキャッシュサーバが、再帰的問い合わせの過程でセカンダリサーバから応答を得ると、不在証明に失敗する。

BIND が NSEC3 をサポートしたのは 9.6 からであり、それより前のバージョンのネームサーバは NSEC3 による不在応答を行えない。

この問題が発生するのは、存在しない名前を解決しようとした場合、つまりこの問題が発生するか否かに関わらず名前解決には失敗する場合であって、その内訳が SERVFAIL か NXDOMAIN かの差異はスタブレゾルバ、あるいはクライアントの動作には相対的に見て大きな影響を与えない。

RedHat Enterprise Linux およびその互換 OS のリリース 6 では bind という名称の RPM パッケージでは BIND 9.7 が提供され、また 5.6 でも bind とは別に bind97 という名称の RPM パッケージで BIND 9.7 が提供されているので、OS をリリース 6 にアップグレードしたり、bind から bind97 に RPM パッケージへ入れ替えることにより、ソースコードから BIND をインストールすることなく RPM パッケージを使い続けたまま、ここで示した問題を回避することができる。

しかしながら、実運用中のサーバのソフトウェアを入れ替えたり OS をアップグレードすることは大きな工数を要すること、とりわけ該当する実装の 1 つである CentOS は、6.0 がリリースされてから日が浅いことから、該当するバージョンのソフトウェアで運用され続けるサーバも当面の間は残ると考えられるので、運用者に注意を喚起する次第である。

セカンダリサーバで、何らかの理由で BIND 9.3 以前を使い続け、かつ dnssec-enable を yes に設定しないのであれば、プライマリサーバの運用者には当該ゾーンで DNSSEC を有効にしてはならないことを周知する必要がある。

セカンダリサーバで、何らかの理由で BIND 9.3 あるいは 9.4 を使い続け、dnssec-enable は yes に設定できるのであれば、プライマリサーバの運用者に、当該ゾーンで DNSSEC を有効にするときには、不在証明の方式として NSEC3 ではなく NSEC を採用するよう周知する必要がある。

以上

※注意事項

・免責事項

本ガイドラインの内容は保証されたものではございません。下記 Web サイトの免責事項をご確認頂き、本ガイドラインを使用してください。

http://dnssec.jp/?page_id=16

・問合せ先

本ガイドラインに関する改善点等のコメントは下記事務局までご連絡頂けると幸いです。

DNSSEC ジャパン事務局　＜sec@dnssec.jp＞