平成 28 年 10 月 5 日

Topic

BIND の脆弱性（CVE-2016-2776）を標的とした無差別な攻撃活動の観測について

DNS サーバのソフトウェアである BIND の脆弱性（CVE-2016-2776）を標的とするアクセスを観測しました。脆弱性の影響を受ける BIND に対する無差別な攻撃活動が実施されている可能性があるため、DNS サーバの管理者等は影響有無の確認及び適切な対策を、早急に実施することを推奨します。

1 BIND の脆弱性（CVE-2016-2776）を標的とした無差別な攻撃活動の観測について

BIND は広く利用されている DNS サーバのソフトウェアです。この BIND について、平成 28 年9月 27 日に開発元から深刻な脆弱性（CVE-2016-2776）が公表[i]されました。また、日本国内の複数の組織からも、当該脆弱性が公表された旨及びインターネット上に当該脆弱性を悪用する攻撃ツールが公開されている旨の注意喚起が順次公表[ii]されました。当該脆弱性が悪用された場合、細工したDNSリクエストを送信するだけで、BINDを異常終了させ、DNS サーバを動作停止させることが可能であるとされています。

10 月4日 18 時以降、警察庁の定点観測システムにおいて、当該脆弱性を標的としたアクセスを観測しました（図1）。

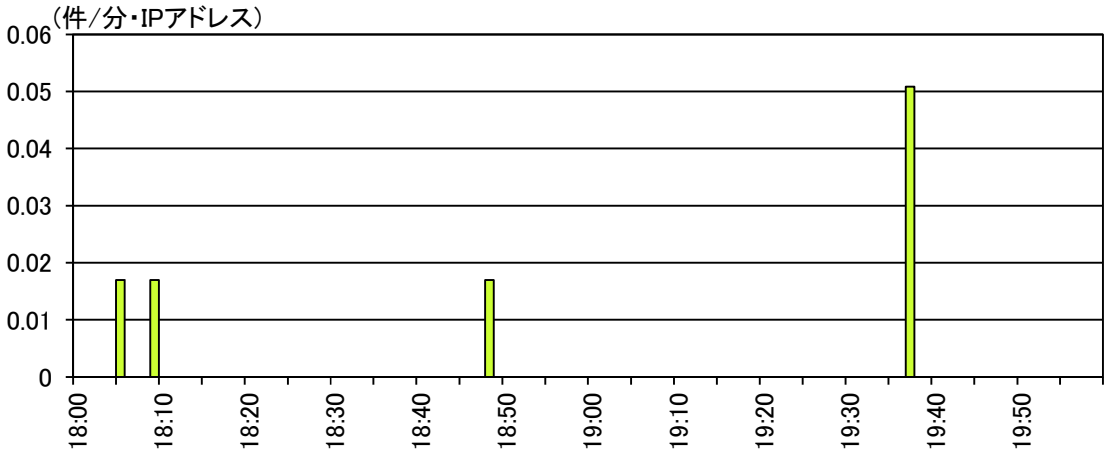

図1 BIND の脆弱性（CVE-2016-2776）を標的とするアクセス件数の推移
（10 月4日 18 時～20 時）

[i] https://kb.isc.org/article/AA-01419/

[ii] 株式会社日本レジストリサービス
https://jprs.jp/tech/security/2016-09-28-bind9-vuln-rendering.html
一般社団法人 JPCERT コーディネーションセンター
https://www.jpcert.or.jp/at/2016/at160037.html
独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/ciadr/vul/20160929-bind.html

観測したアクセスは、宛先ポート 53/UDP に対して細工された DNS リクエストを送信するものでした。また、そのリクエスト内容は、インターネット上に公開されている攻撃ツールを動作させた際に送信される内容と酷似していました。具体的には、攻撃ツールを動作させた際に送信される内容に加えて、更に末尾に1バイトのデータが付加された内容が送信されていました(図2)。

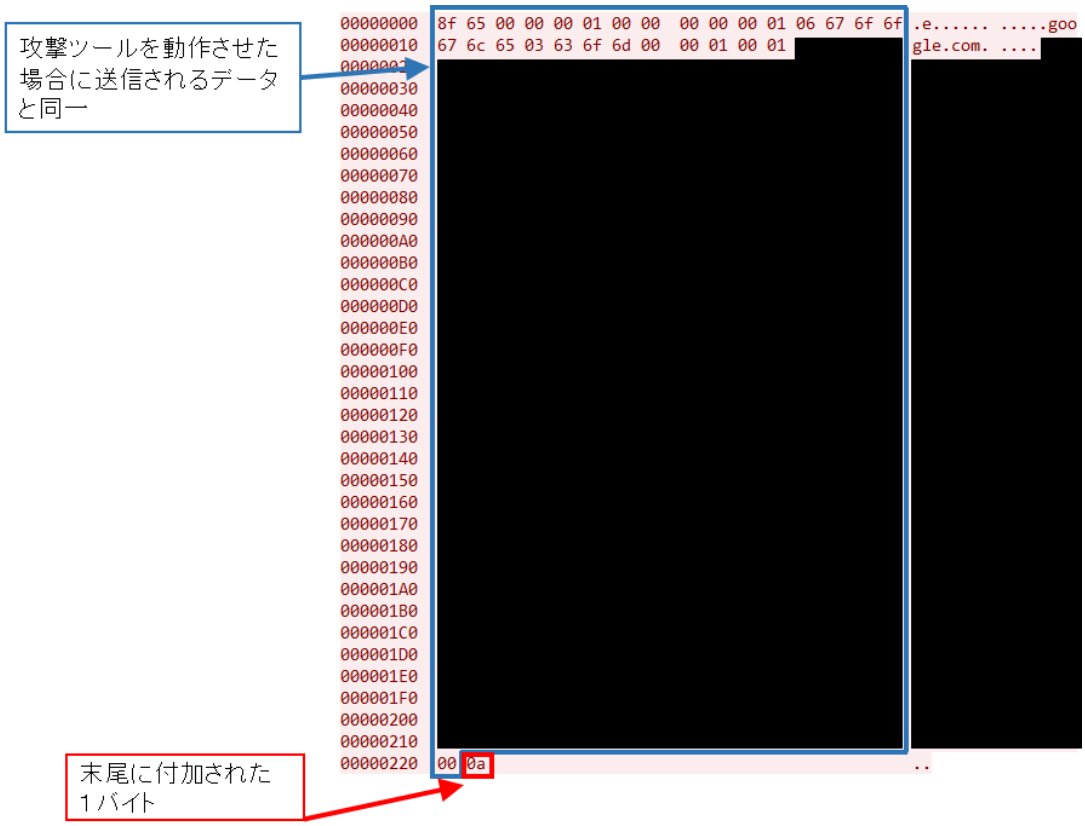

図2　観測したアクセスのリクエスト内容(一部マスキングを実施)

警察庁において検証を実施した結果、末尾に 1 バイトが付加された当該リクエストを受信した際にも、脆弱性の影響を受ける BIND が異常終了することを確認しています。このことから、BIND の異常終了を企図する無差別な攻撃活動が行われていると考えられます。

また、当該アクセスの発信元 IP アドレスは全て相違しており、通常のアクセスにおいてはありえないプライベートアドレスが発信元となっているアクセスも存在するため、当該アクセスの発信元 IP アドレスは詐称されていると考えられます。

2　推奨する対策

BIND を使用して DNS サーバを運用している管理者は以下の対策を早急に実施することを推奨します。

- 使用している BIND が当該脆弱性の影響を受けるバージョンではないか確認を実施してください。
- 使用している BIND が当該脆弱性の影響を受けるバージョンであった場合は、対策済みの最新バージョンにアップデートしてください。

また、当該脆弱性に関する対策等を検討する際は、以下の事項に留意してください。

- キャッシュ DNS サーバ及び権威 DNS サーバ（DNS コンテンツサーバ）の双方が当該脆弱性の影響を受けます。
- 開発元によると、設定変更等による一時的な回避策は存在しません。
- 開発元によると、BIND の設定（allow-query 等）により特定の発信元 IP アドレスからのリクエストのみを許可する設定にしていても、攻撃を回避することはできないとされています。BIND の設定に依存したアクセス制限による回避策は実施しないでください。
- 当該脆弱性を悪用する攻撃リクエストは単一の UDP パケットで実現可能であり、発信元 IP アドレスは容易に詐称可能です。ファイアーウォール等において、発信元 IP アドレスによるアクセス制限を実施していても、発信元 IP アドレスが詐称されることにより、このアクセス制限を回避される可能性があることに留意してください。
- 一般的なサーバ以外にも、DNS サーバの機能を実装するため BIND が組み込まれている機器が存在します。この様な製品を利用している場合には、当該製品の開発元から対策方法等が公表されていないか確認してください。