平成 26 年4月 10 日

Topic

OpenSSL の脆弱性を標的としたアクセスの増加について

OpenSSL において、プロセスのメモリ内容が外部から取得され、秘密鍵などの情報が漏えいする可能性がある深刻な脆弱性が明らかとなりました。同ライブラリを利用している組織においては、アップデートの実施等の適切な対策を早急に実施することを推奨します。

1 OpenSSL の脆弱性を標的としたアクセスの増加について

平成 26 年4月6日に、オープンソースの SSL/TLS ライブラリである OpenSSL の特定のバージョンにおいて、深刻な脆弱性[1]が明らかとなりました。同脆弱性が悪用された場合には、外部から細工したパケットを送信するだけでプロセスのメモリ内容が取得され、秘密鍵などの重要な情報が漏えいする可能性があります。8日には、脆弱性の有無を確認することが可能な攻撃コードも公開されています。

警察庁の定点観測システムにおいても、9日以降、当該攻撃コードに実装されている Client Hello パケット[2]と、完全に一致するパケットを多数観測しています。このことから、同攻撃コードを使用して、脆弱性が存在するサーバ等の探索が実施されているものと考えられます。

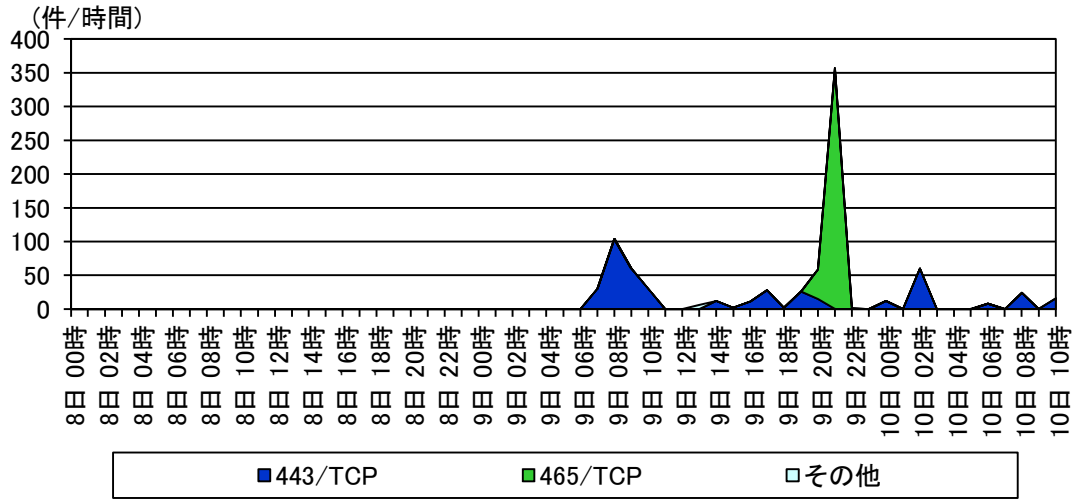

図1 攻撃コードに実装されている Client Hello パケットの宛先ポート別検知件数
（H26.4.8 00:00～H26.4.10 10:59）

[1] 「JVNVU#94401838 OpenSSL の heartbeat 拡張に情報漏えいの脆弱性」（平成 26 年4月8日）
http://jvn.jp/vu/JVNVU94401838/

[2] SSL/TLS 通信において、TCP3ウェイハンドシェイク確立後、クライアントからサーバに対して送信される最初のパケット。

2 推奨する対策

各組織においては、以下の対策を早急に実施することを推奨します。

(1) 該当製品の確認

オープンソースである OpenSSL を使用している製品は多岐に渡ります。各組織で使用している製品に、脆弱性が存在するバージョンの OpenSSL を使用している製品が存在しないか確認を実施してください。

(2) アップデートの実施

脆弱性が存在する OpenSSL を使用しており、OpenSSL ライブラリをアップデート可能な場合には、速やかにアップデートを実施してください。製造元の対応が必要な場合は、各社の対応状況を確認し、アップデートが公開された場合には、速やかに適用を実施してください。

(3) 証明書の失効及び再発行

脆弱性が存在する状態で、SSL 証明書を外部に公開していた場合には、既に秘密鍵が漏えいしている可能性があります。現在使用している証明書を失効させ、再発行することを推奨します。