Cisco Event Response: OpenSSL Heartbleed Vulnerability CVE-2014-0160

脅威の概要：2014 年 4 月 22 日

本文書の内容は、heartbleed.com で公開されている OpenSSL Heartbleed の脆弱性に基づいています。

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

Cisco Security Intelligence Operations

イベント インテリジェンス

以下に、本イベント レスポンス ページに関連するシスコ コンテンツを示します。

シスコ セキュリティ アドバイザリ：複数のシスコ製品における OpenSSL ハートビート拡張の脆弱性
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

Cisco IntelliShield Alert：OpenSSL TLS/DTLS Heartbeat の情報開示の脆弱性
http://tools.cisco.com/security/center/viewThreatOutbreakAlert.x?alertId=33695

Sourcefire VRT ブログへの投稿
http://vrt-blog.snort.org/2014/04/heartbleed-memory-disclosure-upgrade.html

Heartbleed Continued OpenSSL client.html
http://vrt-blog.snort.org/2014/04/heartbleed-continued-openssl-client.html

シスコのセキュリティ ブログへの投稿
http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations
http://blogs.cisco.com/security/cisco-ips-signature-coverage-for-openssl-heartbleed-issue
http://blogs.cisco.com/security/heartbleed-transparency-for-our-customers

脆弱性の特性

OpenSSL Heartbleed の脆弱性には、Common Vulnerabilities and Exposure（CVE）ID CVE-2014-0160 が割り当てられています。

この脆弱性は、TLS ハートビート拡張（RFC6520）の実装、および SSL 対応のサーバが応答を行うためにハートビート要求を検証する方法を不正利用するものです。この脆弱性によって、不適切な長さを持つハートビート要求を巧妙に作成した攻撃者が、ヒープ メモリに格納されている機密情報を含む応答を受信できる可能性があります。複数の要求によって、TLS 暗号通信から情報漏洩が発生する可能性があります。

詳細については、Sourcefire Vulnerability Research Team（VRT）による分析を参照してください。

Cisco Security Intelligence Operations による分析

この攻撃が基盤とするものは単純です。つまり入力検証です。ハートビート要求の長さがチェックされないことによって、範囲外のデータがハートビート応答内に含まれる可能性があります。攻撃者が執拗に複数のメッセージを送信し、SSL 通信から秘密鍵、証明書、個人情報を取得する可能性があります。

内部でのテストでは TLS 通信において、Sourcefire VRT は、ユーザ名、パスワード、SSL 証明書を取得することが可能でした。

シスコ製品への影響

現在、Cisco Product Security Incident Response Team（PSIRT）が、この脆弱性によって影響を受けるシスコ製品を調査中です。公開済みのシスコ セキュリティ アドバイザリ『複数のシスコ製品における OpenSSL ハートビート拡張の脆弱性』には、脆弱性がある製品と、脆弱性がないと確認された製品に関する情報が記載されています。このアドバイザリの内容は、他の製品に関する情報が新たに公開できるようになった際に更新される予定です。シスコは、これらの脆弱性に対応するための無償ソフトウェア アップデートをリリースする予定です。シスコ製品と関連のある最新情報はすべて、Cisco Security Vulnerability Policy に基づいて今後もお伝えしていく予定です。

Cisco Computer Security Incident Response Team（CSIRT）は、この脆弱性の修復を進めるため、本脆弱性の影響を受けやすいと思われるシスコの公開されたインフラストラクチャを調査中です。

緩和策の概要

Cisco Sourcefire Next-Generation Intrusion Prevention System（NGIPS）のイベント アクションを効果的に利用することによって、 この脆弱性を不正利用しようとする攻撃を可視化し、防御することができます。この脆弱性の Sourcefire Snort SID は *30510* *30517* です。これらの Snort SID は、最初のリリース（2014 年 4 月 8 日）以降、有効でわかりやすい検知を実現するために VRT チームによって更新されています。VRT は、OpenSSL クライアントに対する不正利用の試みに関するシグニチャ *30520* *30523* も作成しています。

Cisco Intrusion Prevention System（IPS）を効果的に利用することによって、 この脆弱性を不正利用しようとする攻撃を可視化し、防御することができます。本脆弱性用に作成された、Cisco IPS の対応するシグニチャ ID は 4187/0 および 4187/1 です。 これらのシグニチャは、Cisco IPS Signature Update Package S785（2014 年 4 月 9 日）に含まれていました。Cisco IPS Signature Update Package S786（2014 年 4 月 10 日）以降からは、どちらのシグニチャも検知されることはありません。管理者がこれらのシグニチャのいずれかを個別に使用したい場合、そのシグニチャを新しいシグニチャにコピーし、必要に応じてアクションとフィルタを設定する必要があります。4187/0 は、公開されている概念実証コードによって送信された不正なハートビート要求を検出しますのでご注意ください。シグニチャ 4187/1 は、ハートビート要求に対するサーバの応答が 200 バイト以上のデータを含んでいる場合、その応答を検出します。このシグニチャを使用すると、誤検出によってセンサーに悪影響が及ぼされる可能性があります。そのため、どちらの Cisco IPS シグニチャも、デフォ

ルトでは Retired および Disabled の状態になっています。処理を実行させるには、ネットワーク管理者がこれらのシグニチャを Active かつ Enabled にする必要があります。 信頼性を犠牲にして（フォールス ネガティブ） 4187/1の検知頻度を下げるよう調整するために、ネットワーク管理者は次のような設定を行うことができます。

- 環境のベースラインに基づいて、イベント カウントおよびアラート間隔を高く設定できます。
- バイト チェックの正規表現を、その環境の通常のハートビート要求のサイズに応じて調整することができます。本シグニチャのデフォルトは、 200（16 進数では 0x2c）バイトです。たとえば、300 （16 進数では 0x12c）バイト以上とマッチングするには、本シグニチャの正規表現を（([¥x02-¥xff])|([¥x01][¥x2c-¥xff])）に変更する必要があります。1000（16 進数では 0x3e8）バイトの場合は、 （([¥x04-¥xff])|([¥x03][¥xe8-¥xff])）です。

イベント アクション フィルタを使用して、脆弱性のあるバージョンの OpenSSL を実行していない IP アドレスをシグニチャのアラート対象から除外することも可能です。

Cisco IPS Signature Update Package S786（2014 年 4 月 10 日）は、メタ シグニチャ 4187/2 を導入しました。 これは 4187/0 と 4187/1 を活用したものです。4187/2 は、4187/0 と 4187/1 が検知された時に検知されます。S786 以降、デフォルトで 4187/0 と 4187/1 が独立して検知されることはありません。管理者がこれらのシグニチャのいずれかを個別に使用したい場合、そのシグニチャを新しいシグニチャにコピーし、必要に応じてアクションとフィルタを設定する必要があります。4187/2 は、デフォルトで Retired および Disabled の状態になっています。処理を実行させるには、ネットワーク管理者がこのシグニチャをアクティブかつ有効にする必要があります。

Cisco IPS Signature Update Package S787（2014 年 4 月 15 日）は、シグニチャ 4187/3 および 4187/4 を導入しました。これらはクライアント およびサーバーの不正利用に対する改良された識別を提供します。シグニチャ 4187/3 はクライアントからサーバーへの頻度の高い（２秒間に６回）TLS ハートビートのリクエストを検知します。この頻度は環境に応じて設定を変更することができます。シグニチャ 4187/4 は応答する ハートビート のデータが想定外の大きさかである場合検知します。いずれもデフォルトで Retired および Disabled の状態になっています。処理を実行させるには、ネットワーク管理者がこのシグニチャをアクティブかつ有効にする必要があります。

IPS シグニチャ サブスクリプションを持つすべての Cisco IPS デバイスにて、Unretired および Enabled の状態にした後に、上述のシグニチャを使用できるようになる予定です。

管理者は、攻撃が検出された際にイベント アクションを実行するように IPS センサーを設定できます。設定されたイベント アクションは、攻撃者による Heartbleed の脆弱性の不正利用を防ぐために予防制御または抑止制御を実行します。インライン化されておらず、また悪意のあるパケットをドロップするように設定されていない IPS デバイスは、本脆弱性を不正利用しようとする試みに対してアラートを発生させるだけで、その試みの成功を防ぐ（緩和する）ことはしません。

Cisco Security Manager を使用して、Cisco IPS センサーのアクティビティを表示する方法については、ホワイト ペーパー『Cisco Security Manager を使用した悪意のあるトラフィックの特定』を参照してください。

関連資料

脆弱性ノート VU#720951 http://www.kb.cert.org/vuls/id/720951

CERT-FI アドバイザリ https://www.cert.fi/en/reports/2014/vulnerability788210.html

OpenSSL ニュース https://www.openssl.org/news/secadv_20140407.txt

---

Updated: 2014 年 4 月 30 日

---

http://www.cisco.com/cisco/web/support/JP/112/1122/1122496_ERP-Heartbleed-j.html