TLP: WHITE

ENJOY SAFER TECHNOLOGY™

KR00K - CVE-2019-15126

Wi-Fi 暗号化方式における深刻な脆弱性

筆者：
Miloš Čermák, ESET Malware Researcher
Štefan Svorenčík, ESET Head of Experimental Research and Detection
Róbert Lipovský, ESET Senior Malware Researcher

協力：

Ondrej Kubovič, Security Awareness Specialist

2020 年　2 月

目次

筆者：
Miloš Čermák, ESET Malware Researcher
Štefan Svorenčík, ESET Head of Experimental Research and Detection
Róbert Lipovský, ESET Senior Malware Researcher

協力：

Ondrej Kubovič, Security Awareness Specialist

2020 年　2 月

エグゼクティブサマリー

ESET の研究者は、Wi-Fi チップにこれまで世界に知られていなかった脆弱性を発見し、Kr00k と名付けました。CVE-2019-15126 が割り当てられたこの深刻な脆弱性は、脆弱なデバイスは数字がすべて 0 の暗号化キーを使用して、ユーザーの通信の一部を暗号化するというものです。これを利用した攻撃が成功すると、攻撃者は脆弱なデバイスによって送信された一部のワイヤレスネットワークパケットの解読が可能となってしまいます。

Kr00k は、Broadcom および Cypress による Wi-Fi チップを搭載し、まだパッチが適用されていないデバイスに影響します。これらの Wi-Fi チップは、スマートフォン、タブレット、ラップトップ、IoT ガジェットなどの最新の Wi-Fi 対応デバイスで使用される最も一般的なものです。

クライアントデバイスだけでなく、Broadcom チップを搭載した Wi-Fi アクセスポイントおよびルーターもこの脆弱性の影響を受け、多くのクライアントデバイスの環境が脆弱になります。

私たちのテストでは、パッチを適用する前に、Amazon（Echo、Kindle）、Apple（iPhone、iPad、MacBook）、Google（Nexus）、Samsung（Galaxy）、Raspberry（Pi 3）、Xiaomi（RedMi）の一部のクライアントデバイス及び、Asus と Huawei による一部のアクセスポイントが、Kr00k に対して脆弱であることを確認しました。控えめな見積もりでも、合計で 10 億を超える Wi-Fi 対応デバイスとアクセスポイントが対象となります。さらに、私たちがテストしなかった製品でも、他の多くのベンダーが、この影響を受けるチップセットをデバイスで使用しているはずです。

この脆弱性は、AES-CCMP 暗号化により、WPA2-Personal および WPA2-Enterprise プロトコルの両方に影響を及ぼします。

Kr00k は、2017 年に Mathy Vanhoef によって発見された KRACK（Key Reinstallation Attacks）に関連していますが、根本的に異なります。調査の始めに、Kr00k が、KRACK 攻撃のテストで観察された、数字がすべて 0 の暗号化キーの再インストールに関連して存在することがわかりました。

この脆弱性はチップメーカーである Broadcom とサイプレスに責任を持って開示しました。また、インターネット上のセキュリティの向上のための業界コンソーシアム（ICASI）と協力して、影響を受ける可能性のあるすべての関係者（該当するチップを使用するデバイスメーカーや、影響を受ける可能性のあるその他のチップメーカーなど）が Kr00k を確実に認識できるようにしました。

弊社の情報によると、現在、主要メーカーによるデバイス用のパッチがリリースされています。ユーザーとして自分自身を保護するために、スマートフォン、タブレット、ラップトップ、Wi-Fi 対応の IoT デバイス、Wi-Fi アクセスポイントとルーターなど、すべての Wi-Fi 対応デバイスに利用可能な最新のアップデートを適用してください。デバイスメーカーとして、Kr00k 脆弱性に対するパッチについて、チップメーカーに直接お問い合わせください。

序章

このホワイトペーパーでは、正式に CVE-2019-15126 として知られる Wi-Fi チップの重大な脆弱性である Kr00k を紹介します。

脆弱性のメカニズムとそれに関連する問題について詳述し、Kr00k が攻撃者によって悪用される可能性のある方法のいくつかを示しています。まとめのセクションでは、セキュリティパッチの状態と、組織とユーザーがこの問題に対処する方法について説明します。

IOT を形成する 10 億台を超えるデバイスに潜む欠陥を修正するために、どのような軌跡で報告と開示を実施してきたか、ESET の研究者の発見に至った経緯からお伝えしていきます。

ただし、Kr00k の脆弱性に入る前に、WPA2 セキュリティの簡単な仕組みをご紹介します。この情報は、Kr00k が発生した理由を理解するために必要な前提条件です。

技術的背景

このセクションでは、本書の残りの部分を理解するために必要な、選択された主要な用語の基本的な説明を提供します。

私たちの研究は、*CCMP* をデータの機密性と整合性のプロトコルとして使用する *WPA2* に焦点を当てています。これは、現代の Wi-Fi ネットワークで使用されている最もメジャーな規格です。

クライアントデバイスがアクセスポイントとの接続を確立するたびに、アソシエーションと呼ばれるプロセスが始まります。攻撃は、アソシエーション – **解除** – 再アソシエーションのプロセスを狙います。アソシエーションの再登録のプロセスが何故発生するのか？、これはいくつかの理由があります。

たとえば、信号の干渉が原因で、クライアントがある Wi-Fi アクセスポイントから別の Wi-Fi アクセスポイントにローミングしたとき、または単にユーザーがデバイスの Wi-Fi をオフにしたときです。

アソシエーションと解除は、*管理フレーム*によって管理されます。ここで注意すべき重要な点は、これらは認証も暗号化もされていないということです。そのため、攻撃者は管理フレームを偽造して、ターゲットデバイスによって処理されるアソシエーション解除を手動で発動できます。

WPA2 では、*4 ウェイハンドシェイク*によって安全な通信が確立されます。これにより、クライアントとアクセスポイントの相互認証が保証されます（たとえば、両方が事前共有キー（PSK）、つまり接続デバイスが Wi-Fi アクセスパスワードを既知であることを確認します）。 4 ウェイハンドシェイク中に、クライアントとアクセスポイントは、データの機密性と整合性のために暗号化キーを作成してインストールします。必要とされるキーの 1 つは PTK（ペアワイズトランジェントキー）で、それ自体がさまざまな目的に使用されるさまざまなキーに分割されています。 Kr00k の説明に最も関連するのは、128 ビット **TK (Temporal Key)** です。これは、クライアント AP セッション中に送信されるユニキャストデータフレームの暗号化に使用されます。本文では、TK と「セッションキー」という用語を同じ意味で使用します。

KR00K 脆弱性の発見

図 1 に、チップレベルでの脆弱性の概要を示します。影響を受けるチップ内部の仕組みを詳細に確認することはできませんが、*CYW4356 チップ仕様*) に基づく回路図から、脆弱性の原因と基本的な概念は確認することができます。

Kr00k は、アソシエーション解除後に現れます。①ステーションの WLAN セッションの関連付けが解除されると、②ワイヤレスネットワークインターフェイスコントローラー (WNIC) の Wi-Fi チップに保存されているセッションキー (TK) がメモリから消去され、ゼロに設定されます。アソシエーション解除後にデータが送信されることはないため、これは設計上、予想される動作です。

ただし、③チップの TX（送信）バッファーに残されたすべてのデータフレームは、④すべてゼロのキーで暗号化された後に送信されていました。

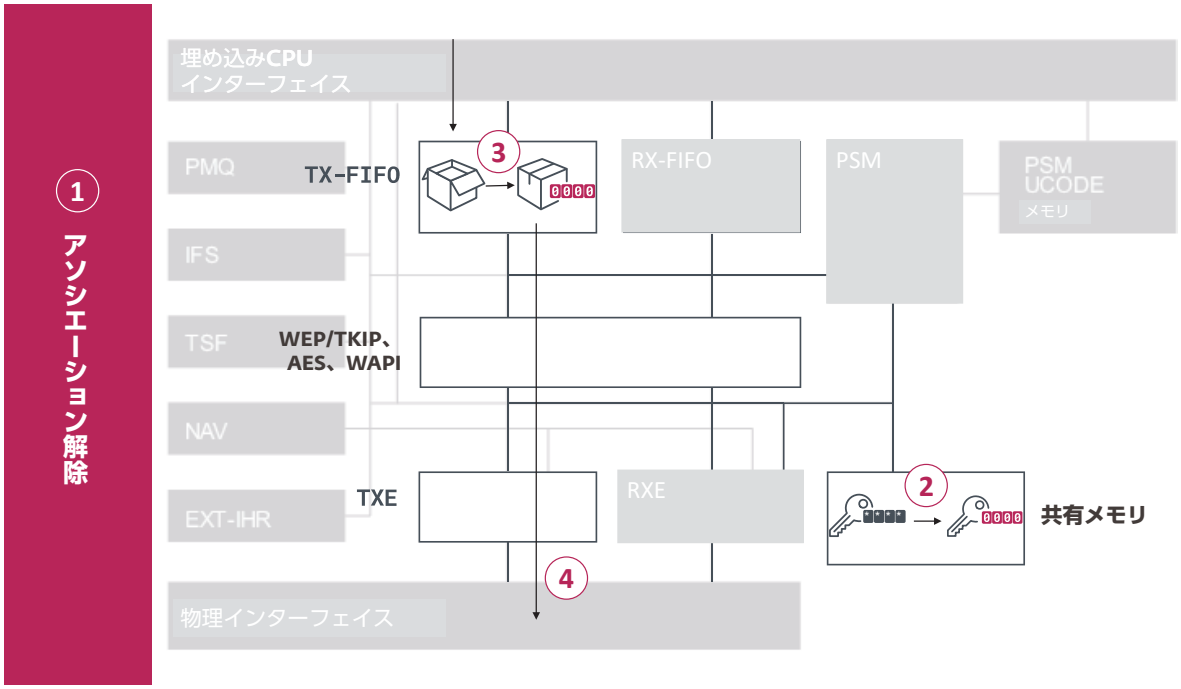


図 1 - kr00k により、すべてゼロのキーで暗号化されたデータが送信されます。

侵入経路：脆弱性の悪用

Kr00k（すべて 0 の TK を使用した暗号化）はアソシエーション解除後に発生させるため、攻撃者は手動で解除を発動させる必要があります。

アソシエーション解除のやり方ですが、認証および暗号化されていない管理データフレームを発動させるのです。例えば不正なパケット、*EAPOL* などの送信などが一例です。

不正な読み取り - データの暗号化

前のセクションで説明したように、アソシエーションが解除されると、チップの TX バッファーからのデータは、すべて 0 の TK で暗号化されて送信されます。これらのデータフレームは、攻撃者によってキャプチャされ、その後復号化されます。このデータには、数キロバイトの機密情報が含まれる可能性があります。

これは、攻撃者が WLAN に接続（認証および関連付け）されていない（たとえば、PSK を知らない）場合でも、*監視モード*で WNIC を使用することにより可能です。

アソシエーション解除を繰り返し発動することにより（セッションは通常自動で再接続されるため、実質的にアソシエーションが繰り返し発生します）、攻撃者はより多くのデータフレームをキャプチャできます。

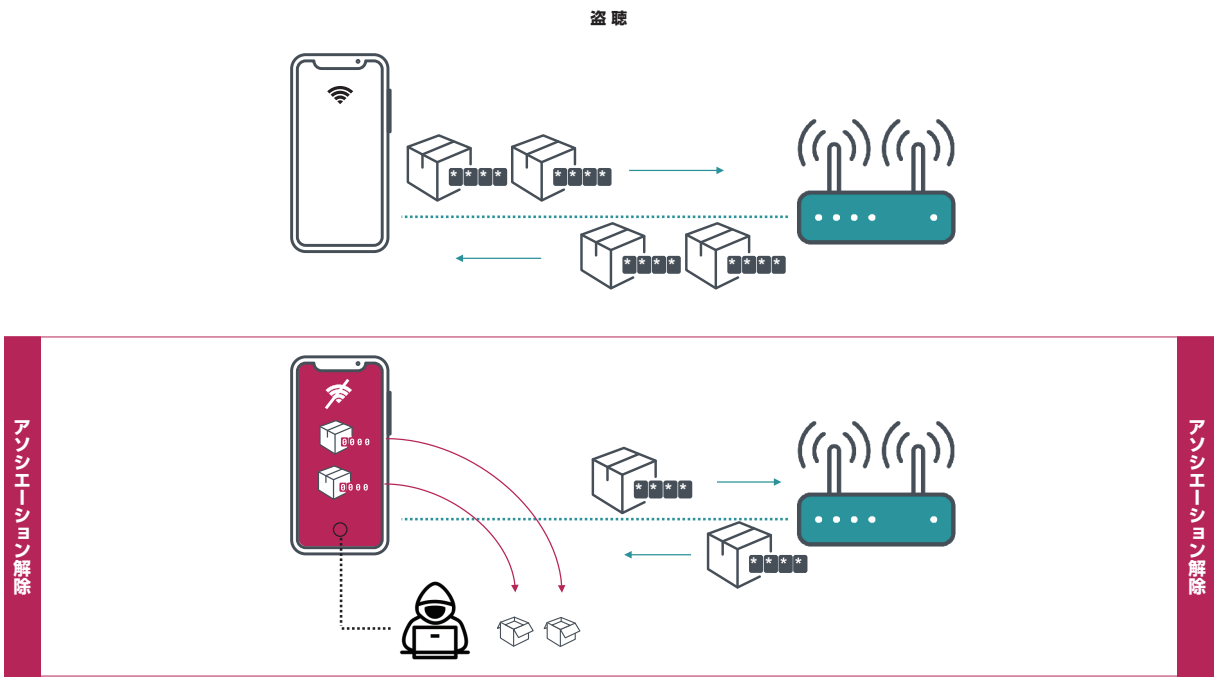
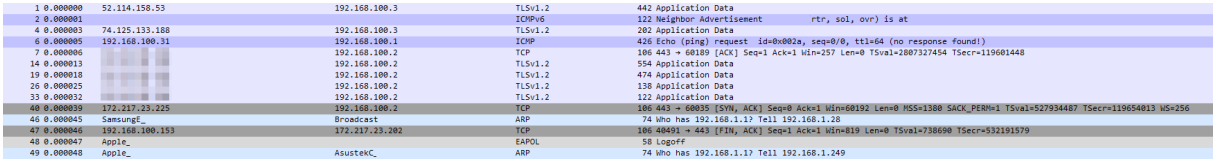


図 2 - 攻撃者は、アソシエーションを解除して、データをキャプチャして復号化します。

その結果、攻撃者は、DNS、ARP、ICMP、HTTP、TCP、TLS パケットなど、機密性の高いデータを含むネットワークパケットをさらにキャプチャできます。これは、WPA2 を使用しないオープンな WLAN ネットワークで見られるものと類似しています。（もちろん、TLS は、この攻撃の影響を受けない暗号化の別のレイヤーを提供します。）



1	0.000000	52.114.158.53	192.168.100.3	TLSv1.2	442 Application Data
2	0.000001			ICMPv6	122 Neighbor Advertisement rtr, sol, ovr) is at
4	0.000003	74.125.133.188	192.168.100.3	TLSv1.2	202 Application Data
6	0.000005	192.168.100.31	192.168.100.1	ICMP	426 Echo (ping) request id=0x002a, seq=0/0, ttl=64 (no response found!)
7	0.000006	[redacted]	192.168.100.2	TCP	106 443 → 60189 [ACK] Seq=1 Ack=1 Win=257 Len=0 TSval=2807327454 TSecr=119601448
14	0.000013	[redacted]	192.168.100.2	TLSv1.2	554 Application Data
19	0.000018	[redacted]	192.168.100.2	TLSv1.2	474 Application Data
26	0.000025	[redacted]	192.168.100.2	TLSv1.2	138 Application Data
33	0.000032	[redacted]	192.168.100.2	TLSv1.2	122 Application Data
40	0.000039	172.217.23.225	192.168.100.2	TCP	106 443 → 60035 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=527934487 TSecr=119654013 WS=256
46	0.000045	SamsungE_	Broadcast	ARP	74 Who has 192.168.1.1? Tell 192.168.1.28
47	0.000046	192.168.100.153	172.217.23.202	TCP	106 40491 → 443 [FIN, ACK] Seq=1 Ack=1 Win=819 Len=0 TSval=738690 TSecr=532191579
48	0.000047	Apple_		EAPOL	58 Logoff
49	0.000048	Apple_	AsustekC_	ARP	74 Who has 192.168.1.1? Tell 192.168.1.249

図 3 - Kr00k の脆弱性により漏えいした WLAN トラフィックの例

影響を受ける機器

この脆弱性は、主に Broadcom とサイプレスが製造した FullMAC WLAN チップに影響を及ぼします。これらのチップメーカーは現在高い市場シェアを持っています。Broadcom チップは世界の市場の Wi-Fi 対応デバイスの大部分で使用されていると言っても間違いありません。サイプレスチップは IoT デバイスで広く使用されています。私たちのラボで Kr00k に対して脆弱であることが明確に確認されたクライアントデバイスは次のとおりです。

- Amazon Echo 2nd gen
- Amazon Kindle 8th gen
- Apple iPad mini 2
- Apple iPhone 6, 6S, 8, XR
- Apple MacBook Air Retina 13-inch 2018
- Google Nexus 5
- Google Nexus 6
- Google Nexus 6P
- Raspberry Pi 3
- Samsung Galaxy S4 GT-I9505
- Samsung Galaxy S8
- Xiaomi Redmi 3S

影響を受けるデバイスの数は、パッチを適用する前は 10 億をはるかに超えていたと推定しています。

Qualcomm、Realtek、Ralink、Mediatek など、他のメーカーの Wi-Fi チップを搭載した一部のデバイスもテストしましたが、脆弱性自体は確認されていません。すべてのメーカーの Wi-Fi チップをテストしたわけではないため、現在影響を受ける他のチップは他にもあるかもしれません。

脆弱なアクセスポイント

クライアントデバイスだけでなく、Wi-Fi アクセスポイントとルーターも Kr00k の影響を受けるリスクが存在します。

これにより、影響を受けないクライアントデバイス（パッチが適用されているか、Kr00k に対して脆弱ではないさまざまな Wi-Fi チップを使用している）が、脆弱であるアクセスポイントに（多くの場合、個人の制御を超えて）接続されます。攻撃者は、脆弱なアクセスポイントから特定のクライアントに送信されたデータを復号化できるため、攻撃対象が大幅に増加することになります。

私たちのラボでは、ASUS と Huawei の一部のワイヤレスルーターが脆弱であることを確認しました：

- Asus RT-N12
- Huawei B612S-25d
- Huawei EchoLife HG8245H
- Huawei E5577Cs-321

KR00K と KRACK の関係

チップセットレベルの Kr00k の脆弱性の発見は、KRACK（Key Reinstallation Attacks）と呼ばれる以前の調査に基づいています。このセクションでは、Kr00k と KRACK が関連しているが根本的に異なります。研究の背景と、Kr00k と KRACK の比較について説明します。

*KRACK 攻撃*は、WPA2 プロトコルに深刻な弱点を明らかにしました – これらは 2017 年に Mathy Vanhoef によって達成された驚くべき発見でした。

最悪の場合のシナリオでは、Vanhoef の論文で説明されているように、KRACK 攻撃により、さまざまな状況下ですべてゼロの TK が設定される可能性があります。

Kr00k で amazon エコー LED をクラッキングする方法

KRACK が広く注目されてから 2 年たっても、すべてのデバイスに完全にパッチが適用されたわけではありません。たとえば、ESET の IoT 調査チームは、*初代の Amazon Echo が KRACK に対して脆弱である*ことを発見しました。報告の後、Amazon はすぐにパッチを発行しました。

第 2 世代の Amazon Echo は元の KRACK 攻撃の影響を受けなかったものの、KRACK 亜種に対して脆弱であることがわかりました。

この欠陥を Amazon に報告したところ、セキュリティチームとの生産的な話し合いの結果、犯人は実際には第 2 世代のエコーで使用されているサイプレス（Cypress）WLAN チップであることがわかりました。これが Kr00k と命名した脆弱性であり、KRACK テストスクリプトがアソシエーション解除を発動することによって、この脆弱性が明らかになったのです。

脆弱な Broadcom チップとサイプレスチップが広く分布しているため、Kr00k はいたるところで攻撃される状態にありました。

KRACK と Kr00k の比較

上記で説明したように、KRACK と Kr00k は関連しています。さらに、どちらもデータの不正な解読を可能にします。

Kr00k は、KRACK 攻撃のテスト中に観察された、アソシエーション解除に発動する、すべて 0 の TK の再インストールが走る脆弱性です。

2 つの主な違いのいくつかを表 1 に示します。

KRACK	Kr00k
KRACK は、その名前が意味するように、一連の攻撃（エクスプロイト）を示します。	一方、Kr00k は脆弱性（バグ）です。
KRACK の重要なポイントは、キーストリームを取得するために Nonce が再利用されることです。	Kr00k の重要なポイントは、データがすべてゼロのセッションキー（TK）で暗号化されることです。
4 ウェイハンドシェイク中にトリガーされます。	アソシエーション解除の後にトリガーされます。
WPA2 プロトコル自体の実装の欠陥を悪用するため、ほとんどの Wi-Fi 対応デバイスに影響します。	広く普及している Wi-Fi チップ（Broadcom および Cypress）に影響します。

表 1 - KRACK と Kr00k の比較

結論

Kr00k – CVE-2019-15126 は数十億のデバイスに影響を与える脆弱性であり、機密データの漏洩を引き起こし、攻撃者たちに新しい攻撃のドアを開く可能性があります。

脆弱性の発見に続いて、ESET は影響を受けたチップメーカーである Broadcom と Cypress（そして最初は Amazon）に報告し、開示を依頼しました。また、ICASI に連絡して、脆弱性が他の（場合によっては）影響を受ける関係者（脆弱なチップを使用するデバイスメーカーおよび他のチップメーカー）に確実に開示されるようにしました。

バグの原因は Wi-Fi チップにありますが、幸いなことに、ソフトウェアまたはファームウェアのアップデートによって軽減できます。

一部のベンダーの出版物および独自の試験によると、デバイスはこの公開時までに脆弱性に対するパッチを受け取っているはずです。デバイスタイプによっては、最新の OS またはソフトウェアの更新がインストールされていることを確認するだけである場合があります（Android、Apple および Windows デバイス、一部の IoT デバイス）。ただし、ファームウェアの更新が必要な場合があります（アクセスポイント、ルーター、一部の IoT デバイス）。

したがって、ユーザーと組織は Broadcom または Cypress チップを搭載したデバイスを最新のソフトウェアバージョンに更新する必要があります。これには、クライアントデバイスとアクセスポイントの両方が含まれます。 Broadcom またはサイプレスチップを使用している製造元は、デバイスにパッチが適用されていることをベンダーに確認する必要があります。

謝辞

この研究に大きく貢献してくれた同僚の Juraj Bartko と Martin Kaluznik に感謝します。

また、発見につながった KRACK に関する彼の優れた研究について、Mathy Vanhoef に敬意を表したいと思います。

最後に、アマゾン、ブロードコム、サイプレスの報告された問題への対応におけるご協力と、影響を受けるベンダーにできるだけ多くに情報を提供するため、尽力くださった ICASI に感謝したいと思います。

本件について Broadcom は公式声明を公開しています。

「Broadcom は、一部のワイヤレスローカルエリアネットワーク（WLAN）デバイスの潜在的な脆弱性を特定するために ESET が行った優れた取り組みに感謝しています。Broadcom は責任ある開示プロセスを経ることで通知を受け、エンドユーザーを確実に保護するための適切な措置を講じることができました。」

発見のタイムラインと開示の経緯

2018 年第 3 四半期	ESET Research が、Amazon Echo と Amazon Kindle の脆弱性のテストを開始。
2019 年 1 月 9 日	ESET Research が、後に Kr00k であることが判明した脆弱性を Amazon に報告。
2019 年 1 月 12 日	Amazon のセキュリティチームが、報告された問題が再現されたことを確認し、詳細な情報を要求。
2019 年上半期	ESET Research が、脆弱性の原因を調査を継続。
2019 年 7 月 18 日	ESET Research が、Cypress の FullMAC Wi-Fi チップを Kr00k の原因であることを特定し、チップの製造元に連絡。
2019 年 7 月 20 日	Cypress のセキュリティチームは、Kr00k 脆弱性の問題を再現できたことを確認。
2019 年 8 月 14 日	ESET Research が、この脆弱性が Cypress の Wi-Fi チップを搭載している IoT デバイスだけでなく、Broadcom のチップを搭載しているデバイスにも影響することを確認。Broadcom に連絡。
2019 年 8 月 16 日	Broadcom のセキュリティチームが報告された脆弱性を確認。Broadcom は、この脆弱性のパッチを作成および公開するために、脆弱性を一般公開するまでの猶予期間（90 ～ 120 日）を要請し、この要請が許諾された。
2019 年 8 月 17 日	Kr00k に CVE-2019-15126 が割り当てられた。
2019 年第 4 四半期 – 2020 年第 1 四半期	この脆弱性の影響を受ける Broadcom および Cypress の Wi-Fi チップをデバイスで使用しているメーカーに Kr00k のパッチが公開される。
2020 年 1 月 16 日	Kr00k の脆弱性が、広範な開示に向けて ICASI に報告された。
2020 年 2 月 26 日	ESET が、Kr00k の脆弱性を公開。

表 2 - 発見のタイムラインと ESET の開示の経緯

ESET について

ESET® は 30 年にわたり、世界中の企業や消費者向けに業界をリードする IT セキュリティソフトウェアとサービスを開発してきました。ESET は、エンドポイントやモバイルセキュリティから、暗号化や二要素認証まで、高性能でありながら使いやすい、さまざまなソリューションを提供しており、消費者や企業がこれらのテクノロジーを最大限に活用し、安全を確保できるようにしています。ESET は、24 時間 365 日、ユーザーに製品を意識させることなく、保護および監視を行い、リアルタイムでセキュリティを更新し、ユーザーを安全に保ち、業務を円滑に遂行できるようにします。脅威が進化する中で、IT セキュリティ企業も進化する必要があります。ESET は、世界中に R&D 研究開発拠点があり、2003 年以降、実環境で使用されたあらゆるマルウェアを特定しています。ESET は、*100 Virus Bulletin（VB100）* アワードを獲得した最初の IT セキュリティ企業です。詳細については、*www.eset.com* をご覧いただくか、*LinkedIn*、*Facebook*、*Twitter* でフォローしてください。

ENJOY SAFER TECHNOLOGY™