Client-seitige Problemumgehung und Erkennung von Wireless KRACK-Angriffen

Inhalt

Einführung

Am 16. Oktober wurden eine Reihe von Sicherheitslücken, die weithin als KRACK bekannt sind, veröffentlicht, die verschiedene Protokolle betreffen, die in Wi-Fi-Netzwerken verwendet werden. Sie wirken sich auf die in WPA/WPA2-Netzwerken verwendeten Sicherheitsprotokolle aus, die den Datenschutz oder die Integrität von Daten gefährden können, wenn diese über eine Wireless-Verbindung übertragen werden.

Die praktischen Auswirkungen variieren je nach Szenario erheblich. Außerdem sind nicht alle Client-seitigen Implementierungen auf dieselbe Weise betroffen.
Bei den Angriffen werden verschiedene clevere Szenarien für "negative Tests" verwendet, bei denen Zustandsänderungen, die auf den Wireless-Standards nicht ordnungsgemäß definiert sind, getestet werden und in den meisten Fällen nicht ordnungsgemäß von dem betroffenen Gerät behandelt werden. Dies gilt nicht für die Verschlüsselungsalgorithmen zum Schutz von WPA2, sondern für die Art und Weise, wie die Authentifizierungs- und Protokollverhandlungen während der Sicherung der Wireless-Verbindung geführt werden.

Die meisten Schwachstellen-Szenarien wurden für Clients berichtet, bei denen bei einem möglichen typischen Angriff gefälschte APs als "Man in the Middle" zum Abfangen und Einschleusen bestimmter Frames während der Sicherheitsverhandlungen zwischen dem Client und dem echten AP verwendet werden (CVE-2017-13077, CVE-2017-1307, CVE-20 17-13079, CVE-2017-13080, CVE-2017-13081). Im Mittelpunkt dieses Dokuments

Es wurde ein Szenario beschrieben, in dem die AP-Infrastruktur angegriffen wird, die 802.11r (FT) Fast Roaming Services (CVE-2017-1382) bereitstellt, das auf dem kürzlich veröffentlichten AireOS-Code behoben wurde.

Es gibt vier weitere Angriffe auf clientspezifische Protokolle: STK, TDLS, WNM, die nicht direkt

von der AireOS-Infrastruktur unterstützt werden (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-10 88) und nicht in den Anwendungsbereich dieses Dokuments fallen.

In der Praxis könnte ein Angreifer Datenverkehr für die betroffene Sitzung entschlüsseln oder Frames in eine oder zwei Richtungen einwerfen. Sie bietet weder eine Möglichkeit, bereits vorhandenen Datenverkehr vor dem Angriff zu dekodieren, noch einen Mechanismus, um die Verschlüsselungskays aller Geräte in einer bestimmten SSID oder ihrem PSK oder 802.1x-Kennwörter "abzurufen".

Die Schwachstellen sind real und haben erhebliche Auswirkungen, aber sie bedeuten nicht, dass WPA2-geschützte Netzwerke "für immer betroffen" sind, da das Problem durch die Verbesserung der Implementierungen auf Client- und AP-Seite behoben werden kann, um in *negativen Testszenarien* ordnungsgemäß zu funktionieren, die derzeit nicht robust gehandhabt werden

Was sollte ein Kunde tun?

- Für Schwachstellen auf Seiten des Access Points: Bei Verwendung von FT wird eine Aktualisierung empfohlen. Wenn FT für Sprach-/Videodienste nicht benötigt wird, prüfen Sie, ob die FT-Funktion deaktiviert werden sollte, bis das Upgrade auf festen Code abgeschlossen ist. Wenn Sie Sprachfunktionen verwenden, prüfen Sie, ob CCKM machbar ist (Client-seitige Unterstützung erforderlich), oder aktualisieren Sie auf festen Code. Wenn kein FT/802.11r verwendet wird, ist derzeit kein Upgrade erforderlich.
- Bei clientseitigen Schwachstellen verbessern Sie Ihre Transparenz: stellen sicher, dass die Erkennung von nicht autorisierten Zugriffen aktiviert ist und alle Kanäle abdeckt, und es wird eine Regel erstellt, "verwaltete SSID" als schädlich zu melden. Implementieren Sie außerdem EAPoL-Konfigurationsänderungen für Wiederholungen, die die auszuführenden Angriffe einschränken oder ganz blockieren können, wie in diesem Dokument beschrieben.

Der Hauptreferenz-Ratgeber finden Sie unter https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. T

Verwendete Komponenten

In diesem Dokument wird der Schwerpunkt auf Wireless-Controllern mit Version 8.0 oder höher gelegt.

Anforderungen

Die Kenntnis der Inhalte, die von dem oben genannten Sicherheitsratgeber abgedeckt werden, ist erforderlich.

Für die WPA KRACK-Angriffe können wir zwei Hauptmaßnahmen ergreifen, um die Clients zu schützen, die noch nicht gepatcht wurden.

1. EAPoL (EAP over LAN)-Wiederholungsschutz

2. Funktionen zur Erkennung von nicht autorisierten Zugriffen und Identitätswechsel von Access Points, um festzustellen, ob die Angriffstools verwendet werden.

Schutz vor EAPoL-Angriffen

Bei Schwachstellen-2017-13077 bis 81 ist es relativ einfach, Clients zu hindern, davon betroffen zu sein, indem ein EAPoL-Wiederholungszähler auf null gesetzt wird. Diese Konfiguration ist in allen WLC-Versionen verfügbar.

Warum funktioniert das?

Für den Angriff ist mindestens ein zusätzlicher EAPoL-Wiederholungsversuch erforderlich, der vom Authentifizierer während des 4-Wege-Handshake oder während der Rotation des Sendeschlüssels generiert wurde. Wenn wir die Generierung von Wiederholungen blockieren, kann der Angriff nicht gegen einen Pairwise Transient Key (PTK)/Groupwise Transient Key (GTK) angewendet werden.

Mögliche Auswirkungen

1. Clients, die langsam sind oder die erste Verarbeitung von EAPoL M1 verwerfen können (d. h. die erste Meldung des 4-Wege-Tastenaustauschs). Dies wird bei einigen kleinen Clients oder Telefonen beobachtet, die möglicherweise den M1 erhalten und nach der 802.1x-Authentifizierungsphase nicht zur Verarbeitung bereit sind, oder wenn dies zu langsam geschieht, um einen kurzen Wiederübertragungs-Timer zu erfüllen

2. Szenarien mit schlechter Funkumgebung oder WAN-Verbindungen zwischen AP und WLC, die zu einem Paketverlust bei der Übertragung an den Client führen können.

In beiden Szenarien besteht das Ergebnis darin, dass ein EAPoL-Exchange-Fehler gemeldet und der Client deauthentifiziert wird. Die Assoziations- und Authentifizierungsprozesse müssen neu gestartet werden.

Um die Wahrscheinlichkeit des Auftretens dieses Problems zu verringern, sollte ein längeres Timeout (1000 ms) verwendet werden, um langsamen Clients mehr Zeit für die Reaktion zu geben. Der Standardwert ist 1000 ms, kann aber manuell in einen niedrigeren Wert geändert worden sein, damit dieser überprüft werden kann.

Konfiguration

Es stehen zwei Mechanismen zur Konfiguration dieser Änderung zur Verfügung.

- Global, verfügbar in allen Versionen
- Pro WLAN, verfügbar ab Version 7.6

Die globale Option ist einfacher und kann in allen Versionen verwendet werden. Die Auswirkungen sind für alle WLANs im WLC sichtbar.

Die WLAN-Konfigurationseinstellungen ermöglichen eine präzisere Steuerung, wobei die betroffenen SSIDs eingeschränkt werden können, sodass die Änderungen je Gerätetyp usw. angewendet werden können, wenn sie in bestimmten WLANs gruppiert werden. Diese Funktion ist in Version 7.6 verfügbar.

Beispielsweise könnte es auf ein generisches 802.1x-WLAN angewendet werden, jedoch nicht auf ein sprachspezifisches WLAN, wo es größere Auswirkungen haben kann

Größte globale Konfig.:

```
config advanced eap eapol-key-retries 0
```

(Nur CLI-Option)

Der Wert kann wie folgt validiert werden:

```
(2500-1-ipv6) >show advanced eap

EAP-Identity-Request Timeout (seconds)..... 30

EAP-Identity-Request Max Retries.............. 2

EAP Key-Index for Dynamic WEP................. 0

EAP Max-Login Ignore Identity Response..... enable

EAP-Request Timeout (seconds)................. 30

EAP-Request Max Retries....................... 2

EAPOL-Key Timeout (milliseconds)............... 1000

EAPOL-Key Max Retries......................... 0

EAP-Broadcast Key Interval..................... 3600
```

Nr. 2 pro WLAN-Konfiguration

X=WLAN-ID

```
config wlan security eap-params enable X

config wlan security eap-params eapol-key-retries 0 X
```

Identifizieren, ob ein Client aufgrund von Neuübertragungen ohne Neuübertragungen gelöscht wird

Der Client wird gelöscht, da maximal EAPoL-Wiederholungen erreicht und deauthentifiziert wurden. Die Anzahl der Neuübertragungen beträgt 1, da der ursprüngliche Frame gezählt wird.

```
 *Dot1x_NW_MsgTask_6: Oct 19 12:44:13.524: 28:34:a2:82:41:f6 Sending EAPOL-Key Message to mobile
28:34:a2:82:41:f6
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
..
*osapiBsnTimer: Oct 19 12:44:14.042: 28:34:a2:82:41:f6 802.1x 'timeoutEvt' Timer expired for
station 28:34:a2:82:41:f6 and for message = M3
*Dot1x_NW_MsgTask_6: Oct 19 12:44:14.042: 28:34:a2:82:41:f6 Retransmit failure for EAPOL-Key M3
to mobile 28:34:a2:82:41:f6, retransmit count 1, mscb deauth count 0
..
*Dot1x_NW_MsgTask_6: Oct 19 12:44:14.043: 28:34:a2:82:41:f6 Sent Deauthenticate to mobile on
BSSID 58:ac:78:89:b4:19 slot 1(caller 1x_ptsm.c:602)
```

Erkennung nicht autorisierter APs

Einige der Angriffstechniken für die Sicherheitslücken gegen die Client-Verschlüsselung PMK/GTK

müssen einen gefälschten AP mit derselben SSID wie der Infrastruktur-AP "darstellen", der jedoch auf einem anderen Kanal betrieben wird. Dies kann problemlos erkannt werden, und der Netzwerkadministrator kann je nach Aktivität physische Maßnahmen ergreifen.

Es gibt bisher zwei Möglichkeiten, EAPoL-Angriffe durchzuführen:

- Anders ausgedrückt: Die Fakturierung von Infrastruktur-APs, die als nicht autorisierter Access Point fungieren und dieselbe MAC-Adresse verwenden, eines echten Access Points, jedoch auf einem anderen Kanal. Einfach für den Angreifer, aber sichtbar
- Einspeisen von Frames in eine gültige Verbindung, sodass der Client reagieren muss. Dies ist viel weniger sichtbar, aber unter bestimmten Umständen erkennbar, es kann sehr sorgfältiges Timing erfordern, um erfolgreich zu sein

Durch die Kombination von Identitätsfunktionen für APs und Erkennung von nicht autorisierten Access Points kann festgestellt werden, ob eine "gefälschte ap" im Netzwerk platziert wird.

Konfiguration

- Überprüfen Sie, ob die Erkennung nicht autorisierter Access Points aktiviert ist. Diese Funktion ist standardmäßig aktiviert, kann aber vom Administrator manuell deaktiviert werden. Sie muss daher überprüft werden.
- Erstellen Sie eine Regel, um unberechtigte Benutzer mithilfe von "verwalteten SSIDs" als schädlich zu kennzeichnen:
- Stellen Sie sicher, dass die Kanalüberwachung für 802.11a/b-Netzwerke auf "alle Kanäle" eingestellt ist. Der Basisangriff ist so konzipiert, dass er sich in der Nähe des Clients befindet, und zwar auf einem anderen Kanal als in den Infrastruktur-APs. Daher ist es wichtig, sicherzustellen, dass alle möglichen Kanäle gescannt werden:

AP-Identitätswechsel

Bei der Standardkonfiguration kann die Infrastruktur erkennen, ob das Angriffstool eine unserer AP-MAC-Adressen verwendet. Dies wird als SNMP-Trap gemeldet und weist darauf hin, dass der Angriff stattfindet.

```
Impersonation of AP with Base Radio MAC bc:16:65:13:a0:40 using source address of
bc:16:65:13:a0:40 has been detected by the AP with MAC Address: bc:16:65:13:a0:40 on its
802.11b/g radio whose slot ID is 0
```

Referenzen

Sicherheitsratgeber

Verwaltung nicht autorisierter APs in einem Unified Wireless Network mit v7.4 - Cisco

Cisco Wireless LAN Controller - Best Practices für die Konfiguration - Cisco

Erkennung nicht autorisierter APs unter Unified Wireless Networks - Cisco