EC-COUNCIL

WPA2 KEY INSTALLATION KRACK ATTACKS: BRIEFING

FROM THE DESK OF KEVIN KING
DIRECTOR TECHNICAL INNOVATION
EC-COUNCIL | GLOBAL

CONTENTS

All about WPA2 Key

Installation KRACK Attack

Threat

CISO Action Guide

User Awareness

References

What is a KRACK Attack?

A new vulnerability has been discovered allowing WiFi networks protected by WPA2 to be attacked, exposing all information transferred between a host and the WAP. It is a KRACK or "Key Reinstallation AttaCK."

The vulnerability has been demonstrated to be effective against Linux-based devices including Linux, Apple iOS, Android 6.0 and above, macOS, and OpenBSD.

Microsoft devices are not affected.

WPA2 KRAK Process (there are several potential variations not covered here)

1. The victim clicks on an HTTPS link or types in an HTTPS URL
2. The attacker clones the target WPA2 network on a different channel so that hand shake messages can be manipulated to take advantages of weaknesses
3. SSLStrip is used to expose HTTPS for improperly configured websites
4. Victim's WiFi connection is bumped to a different channel via the attacker
5. A key re-installation attack Is perpetrated against the 4 way handshake
6. All data is exposed allowing the attacker to capture PIM

The user will likely not notice that he or she is no longer secured under HTTPS and continue to expose data.

The CISO Guide to KRACK Attack vulnerability

- The attack was discovered by Mathy Vanhoef of imec-DistriNet.
- The attack involves a reinstallation of the parewise encryption key (PTK-TK) in the 4-way handshake.
- It can involve the reinstallation of the group key (GTK) or the integrity group key (IGTK) in the 4 way handshake.
- There are other variants.
- This impacts ALL WiFi devices including laptops, notepads, phones, IoT devices like TVs, including IPA WiFi-connected smart devices like Amazon Echo and Google Home

- Avoid public Wi-Fi hot spots until you confirm your device is adequately patched.
- If your Wi-Fi router is not password protected, do so immediately.
- Upload the latest Operating System (OS) to all of your Wi-Fi enabled devices.
- Upload any additional firmware patches your device manufacturer recommends.
- Until you get your device patched, plug it directly into the network with ethernet cable.
- In the meantime, only visit secure websites that use "https" secure protocol.
- Contact any company whose services you use and ask if the connection is secured using TLS 1.2 (if so, your connection with that service is safe for now).
- Use Virtual Private Networks (VPNs), but only vetted, reputable, paid services are advisable (free VPNs can be vulnerable).

VENDOR RESPONSE

Linksys/Belkin

"Belkin Linksys, and Wemo are aware of the WPA vulnerability. Our security teams are verifying details and we will advise accordingly. Also know that we are committed to putting the customer first and are planning to post instructions on our security advisory page on what customers can do to update their products, if and when required."

Apple iOS and Mac

Apple confirmed it has a fix in beta for iOS, MacOS, WatchOS and TVOS, and will be rolling it out in a software update in a few weeks.

Google Mobile

"We're aware of the issue, and we will be patching any affected devices in the coming weeks."

Google Chromecast/ Home/ WiFi

"We're aware of the issue, and we will be patching any affected devices in the coming weeks."

Microsoft

Some companies have already stepped up to patch their devices after the KRACK Wi-Fi security flaw.
James Martin/CNET"Microsoft released security updates on October 10th and customers who have Windows Update enabled and applied the security updates, are protected automatically. We updated to protect customers as soon as possible, but as a responsible industry partner, we withheld disclosure until other vendors could develop and release updates."

Amazon Echo, FireTV and Kindle

"We are in the process of reviewing which of our devices may contain this vulnerability and will be issuing patches where needed."

Samsung Mobile

"As soon as we are notified of any potential vulnerabilities, we work closely to address those issues as quickly as possible. We are aware of this matter and will be rolling out patches to Samsung devices in the coming weeks."

Netgear

"NETGEAR is aware of the recently publicized security exploit KRACK, which takes advantage of security vulnerabilities in WPA2 (WiFi Protected Access II). NETGEAR has published fixes for multiple products and is working on fixes for others. Please follow the security advisory for updates.
"NETGEAR appreciates having security concerns brought to our attention and are constantly monitoring our products to get in front of the latest threats. Being pro-active rather than re-active to emerging security issues is a fundamental belief at NETGEAR.
"To protect users, NETGEAR does not publicly announce security vulnerabilities until fixes are publicly available, nor are the exact details of such vulnerabilities released. Once fixes are available, NETGEAR will announce the vulnerabilities from NETGEAR Product Security web page."

VENDOR RESPONSE Continued..

D-Link

"On Oct. 16, 2017, a WPA2 wireless protocol vulnerability was reported. D-Link immediately took actions to investigate the issues. This appears to be an industry-wide issue that will require firmware patches to be provided from the relevant semiconductor chipset manufacturers. D-Link has requested assistance from the chipset manufacturers. As soon as patches are received and validated from the chipset manufacturers, D-Link will post updates on its website support.dlink.com immediately."

Sprint

"Since Sprint's network operates on CDMA and LTE technology, not Wi-Fi, the KRACK vulnerabilities are not direct threats to those wireless networks. However, similar to any large company that utilizes Wi-Fi for internal business, we have taken steps to address the vulnerability internally to protect the company."

Intel

"Intel was notified by the Industry Consortium for Advancement of Security on the Internet (ICASI) and CERT CC of the identified Wi-Fi Protected Access II (WPA2) standard protocol vulnerability. Intel is an ICASI charter member and is part of the coordinated disclosure of this issue.
"Intel is working with its customers and equipment manufacturers to implement and validate firmware and software updates that address the vulnerability. For more information, please refer to Intel's security advisory on this vulnerability - INTEL-SA-00101"

LG Mobile

"Smartphone OEMs have to work very closely with Google to find solutions for OS-level vulnerabilities.
"Google is in the process of rolling out patches to carriers and manufacturers at this very moment but it takes time to cover all the major smartphone models.
"So it's hard to say exactly when a specific phone will get the fix but it's certainly being addressed."

User Awareness Script

- WiFi Use
- Updates
- HTTPS Connection

Proceed to the next slide for the script.

Dear Colleagues,

Recently, a new weakness has been discovered in WPA2, the protocol used to connect most every WiFi network. This weakness will allow all of the data you transmit from your phone, laptop, tablet, or any WiFi-connected device to be visible to an attacker.

We request you to follow the best practices outlined below while performing your daily operations:

- Update all devices, including IoT devices like TVs and refrigerators.
- Use Microsoft phones and tables where possible.
- Use the Corporate network, not ad-hock WiFi in the area.
- Use cellular data instead of WiFi where you can.
- Purchase and use a VPN like IPVanish, VyprVPN, or HMA when in public
- Always double check your connection to ensure you are securely connected
- Follow the Computer Usage policy. <link to corporate policy>

If you use an Android or Apple device, try to stay off of public Wi-Fi networks for now. If you absolutely must use public Wi-Fi, make sure you stick to secured sites that have HTTPS in their web address. And, of course, hope that Google and Apple roll out their patches soon.

<CISO Signature Block>

REFERENCES

Refernces

- https://www.krackattacks.com/
- https://cwe.mitre.org/data/definitions/323.html
- https://papers.mathyvanhoef.com/ccs2017.pdf
- https://www.kb.cert.org/vuls/id/228519
- https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-security-update
- https://forum.mikrotik.com/viewtopic.php?f=21&t=126695
- https://github.com/vanhoefm/krackattacks-test-ap-ft
- https://twitter.com/vanhoefm/status/920637745768402945
- https://exchange.xforce.ibmcloud.com/collection/396ecb6880625d6e58dd7636b7c8e8fd
- http://appleinsider.com/articles/17/10/16/apple-confirms-krack-wi-fi-wpa-2-attack-vector-patched-in-ios-tvos-watchos-macos-betas
- https://www.theverge.com/2017/10/16/16481818/wi-fi-attack-response-security-patches
- http://www.zdnet.com/article/here-is-every-patch-for-krack-wi-fi-attack-available-right-now/
- https://www.theregister.co.uk/2017/10/16/wpa2_krack_attack_security_wifi_wireless/
- https://arstechnica.com/information-technology/2017/10/how-the-krack-attack-destroys-nearly-all-wi-fi-security/

Vendor Links

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa
- http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt
- http://svn.dd-wrt.com/changeset/33525
- https://github.com/espressif/ESP8266_NONOS_SDK
- https://github.com/espressif/ESP8266_RTOS_SDK
- https://github.com/espressif/esp-idf
- https://w1.fi/security/2017-1/
- https://kb.netgear.com/000049346/WNDAP350-Firmware-Version-3-7-7-0
- https://kb.netgear.com/000049349/WNAP320-Firmware-Version-3-7-7-0
- https://kb.netgear.com/000049353/WAC120-Firmware-Version-2-1-5
- https://kb.netgear.com/000049065/WAC505-WAC510-Firmware-Version-1-5-3-7
- https://kb.netgear.com/000049065/WAC505-WAC510-Firmware-Version-1-5-3-7
- https://kb.netgear.com/000049351/WND930-Firmware-Version-2-1-3
- https://kb.netgear.com/000049345/WNDAP660-Firmware-Version-3-7-7-0
- https://kb.netgear.com/000049348/WNAP210v2-Firmware-Version-3-7-7-0
- https://kb.netgear.com/000049001/WAC720-WAC730-Firmware-Version-3-7-12-0
- https://kb.netgear.com/000049350/WNDAP620-Firmware-Version-2-1-4
- https://kb.netgear.com/000049352/WN604-Firmware-Version-3-3-8
- http://support.toshiba.com/support/staticContentDetail?contentId=4015875&isFromTOCLink=false
- https://community.ubnt.com/t5/UniFi-Updates-Blog/FIRMWARE-3-9-3-7537-for-UAP-USW-has-been-released/ba-p/2099365
- http://www.zyxel.com/support/announcement_wpa2_key_management.shtml
- https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10827&cat=SIRT_1&actp=LIST
- https://usn.ubuntu.com/usn/usn-3455-1/
- http://www.icasi.org/wi-fi-protected-access-wpa-vulnerabilities/
- https://access.redhat.com/errata/RHSA-2017:2907
- https://www.debian.org/security/2017/dsa-3999

DISCLAIMER

This briefing is for informational purposes only and should not be utilized as a solution to the KRACK attack. If you believe you have been affected or have questions on how to remediate, reach out to a security consulting company.