山东省新闻出版广电局

山东省新闻出版广电局
关于做好无线路由防护工作的通知

各市文化广电新闻出版局、淄博市广播电视台，山东广播电视台、山东广电网络有限公司、山东教育电视台，各有关单位:

近日，国家新闻出版广电总局科技司下发《关于无线路由加密协议 WPA2 存在多个漏洞的通报》（技新字〔2017〕547 号），对新近发现的无线路由安全隐患情况进行了通报，并提出工作建议。请各市局、各单位组织辖区内新闻出版广电部门及本单位加强无线路由防护，切实保障网络安全及广播电视播出安全。

附件：国家新闻出版广电总局科技司关于无线路由加密协议 WPA2 存在多个漏洞的通报

山东省新闻出版广电局

2017 年 11 月 15 日

国家新闻出版广电总局(司局函件)

技新字(2017)547号

国家新闻出版广电总局科技司关于无线路由加密协议WPA2存在多个漏洞的通报

各省、自治区、直辖市、新疆生产建设兵团新闻出版广电局，总局直属各单位:

近日，我司收到《无线路由加密协议WPA2存在多个漏洞》（国信安测[2017]第29期）（见附件1）的信息安全漏洞通报，并请相关技术专家对受影响厂商设备、产品型号及补丁链接（见附件2）进行了细化，并提出了以下建议:

1、排查本单位相关设备的生产厂商、产品型号，对存在漏洞的设备按补丁链接及时更新固件和驱动程序，跟踪所部署WiFi设备厂商安全公告;

2、严格遵守保密规定，严禁涉密设备和设施连接WiFi热点;

3、合理部署无线入侵检测/防御系统，加强对已有WiFi管理，及时并定期监测周边恶意钓鱼WiFi，加以阻断干扰，开展定期检查;

4、定期组织安全培训，强化安全意识，不随意连接WiFi热

点。

请各单位及时排查相关设备，采取有效应对措施，确保各系统安全运行。

附件：1.无线路由加密协议WPA2存在多个漏洞.pdf

2.受影响厂商设备、产品型号及补丁链接.docx

国家新闻出版广电总局科技司

2017年11月10日

抄报：总局田进副局长

国家新闻出版广电总局司局　　2017年11月13日印发

信息安全漏洞通报

国信安测〔2017〕第29期

信息安全测评中心　　2017年10月17日

无线路由加密协议WPA2存在多个漏洞

2017年10月16日，比利时鲁汶大学研究员在专门网站https://www.krackattacks.com/称，现有无线（WiFi）路由设备最常使用的协议WPA2，存在多个漏洞。攻击者可在目标WiFi覆盖的范围内使用密钥重装（Key Reinstallation Attack, KRACK）攻击技术，破解WiFi密钥，获取加密的信用卡号、密码、聊天信息、电子邮件、照片等敏感信息，甚至控制无线路由器设备。该网站详述了攻击技术原理，并附有演示视频、10个相关漏洞的CVE预留编号，但未公布漏洞详情、利用代码和相关工具。美国计算机应急响应小组（CERT）已公布了思科、谷歌、英特尔、微软等23家受到漏洞影响的厂商，其中部分厂商已提供相关补丁，修复漏洞或防御攻击。

对策建议

（一）对确认受到影响的厂商，及时升级相关补丁或联系厂商确认修复方案。

（二）加强对单位及周边伪造 WiFi 热点的监控。

（三）严禁涉密设备和设施连接 WiFi 热点，严格遵守保密规定。

（四）加强安全意识，不随意连接 WiFi 热点。

附件：1.KRACK 攻击涉及漏洞列表

2.KRACK 技术原理

3.受影响厂商及相应补丁链接

联系方式：010-82341439

主题词：美国　Netsarang 公司　软件　恶意代码

主送：各部委信息安全主管部门

信息安全测评中心通报处　　2017 年 10 月 18 日印发

（存档 1 份　共印 80 份）

附件 1：KRACK 攻击涉及漏洞列表

CNNVD-201710-380（CVE-2017-13077）：在四次握手中重装成对加密密钥（PTK-TK）
CNNVD-201710-381（CVE-2017-13078）：在四次握手中重装组密钥（GTK）
CNNVD-201710-382（CVE-2017-13079）：在四次握手中重装完整组密钥（IGTK）
CNNVD-201710-383（CVE-2017-13080）：在组密钥握手中重装组密钥（GTK）
CNNVD-201710-384（CVE-2017-13081）：在组密钥握手中重装完整组密钥（IGTK）
CNNVD-201710-385（CVE-2017-13082）：接受重新传输的快速 BSS 切换（FT）重新关联请求，处理的同时重装成对加密密钥（PTK-TK）
CNNVD-201710-386（CVE-2017-13084）：在 PeerKey 握手中重装 STK 密钥
CNNVD-201710-387（CVE-2017-13086）：在 TDLS（Tunneled Direct-Link Setup，通道直接链路建立）握手中重装 TDLS PeerKey（TPK）
CNNVD-201710-388（CVE-2017-13087）：处理无线网络管理（WNM）休眠模式响应帧时重装组密钥（GTK）
CNNVD-201710-389（CVE-2017-13088）：处理无线网络管理（WNM）休眠响应帧时重装完整组密钥（IGTK）

附件 2：技术原理

从网站上提供的攻击原理上分析，KRACK 攻击应该是针对 WPA2 的中间人攻击方法，类似于 DNS 投毒式攻击模式。攻击并不针对 WPA 加密本身，而是通过多次重播四次握手的消息来强制，复位 WiFi 用户所保存的 WPA 密钥，即把原来正确真实的 WPA 密码替换掉，不破解直接替换，这样就可以将受害者连到伪造的 AP 上，无需任何提示，再配合 SSLStrip 之类的证书伪造工具等即可实现不易识别的钓鱼攻击。

其有 3 点特征:

1、其实协议从服务端来看并未被攻破，即 WiFi 路由器设备尚且安全，而是利用了协议本身的缺陷，使得 WiFi 用户存在被攻击的潜在可能;

2、这种攻击模式最直接的利用方式既是伪造 AP，令用户链接到非法的伪造 WiFi 节点上，从而实现后续的钓鱼、嗅探等攻击;

3、由于攻击面向 WiFi 用户，WiFi 路由器设备目前尚未有安全的协议替换或相关补丁可解决此问题。

附件 3：受影响厂商及相应补丁链接

受影响厂商	补丁链接
Aruba Networks	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa
Espressif Systems	https://github.com/espressif/esp-idf https://github.com/espressif/ESP8266_RTOS_SDK https://github.com/espressif/ESP8266_NONOS_SDK
Fortinet, Inc.	http://docs.fortinet.com/uploaded/files/3961/fortiap-v5.6.1-release-notes.pdf
FreeBSD Project	暂无
Google	暂无
HostAP	https://w1.fi/security/2017-1/
Intel Corporation	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00101&languageid=en-fr
Juniper Networks	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10827&actp=METADATA
Microchip Technology	http://www.microchip.com/design-centers/wireless-connectivity/embedded-wi-fi/wpa2-protocol-vulnerability
Microsoft Corporation	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080
OpenBSD	暂无
Peplink	https://forum.peplink.com/t/security-advisory-wpa2-vulnerability-vu-228519/12715
Red Hat, Inc.	暂无
Samsung Mobile	暂无
Sierra Wireless	https://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---wpa-and-wpa2-vulnerabilities/
Toshiba Commerce Solutions	https://tgcs04.toshibacommerce.com/cs/idcplg?IdcService=FLD_BROWSE&path=%2fCommunications%2fSecurity%20Alerts&doMarkSubscribed=1 http://www.toshibacommerce.com/ https://www.toshibacommerce.com/forms/anon/org/app/e8ee98aa-3101-4218-8ac3-1d50c734aa99/launch/index.html?form=F_Form1 https://www.toshibacommerce.com/wps/myportal/%21ut/p/a1/rZRNc8IgEIZ_Sw8eGQhJCDmmWr8abW2dqcnFoYQoTiDRRK399UXrrWOtUzgws7A87y6z88IUzmCq2U4uWCNLzYpjnJJ5-ExR_wnhYa-LAxTRid-j3UcHDTB8gylMuW6qZgkToVtoWSrRQlrs6-8dbEQhWC1MyKqNLABGDjlf1YJvN7I5AF4qtdWSn2TrI7J

附件 2 受影响厂商设备、产品型号及补丁链接

受影响厂商	形态	设备/产品型号	补丁链接
Aruba Networks	设备	Aruba 501 Client Bridge	http://community.arubanetworks.com/t5/Wireless-Access/WPA2-Vulnerability-Discussion/td-p/310066
	软件	Aruba Instant	
	软件	ArubaOS	
CISCO	Endpoint Clients and Client Software	Cisco AnyConnect Secure Mobility Client - Network Access Manager	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa
	Routing and Switching - Small Business	Cisco DX Series IP Phones (DX70 and DX80) when running Collaboration Endpoint (CE) software	
	Voice and Unified Communications Devices	Cisco IP Phone 8861	
		Cisco IP Phone 8865	
		Cisco IP Phone 8865	
		Cisco Spark Room Series	
		Cisco Wireless IP Phone 8821	
	Wireless	Cisco 1100 Series Integrated Services Routers	
		Cisco 812 Series Integrated Services Routers	
		Cisco 819 Series Integrated Services Routers	
		Cisco 829 Industrial Integrated Services Routers	
		Cisco 860 Series Integrated Services Routers	
		Cisco 880 Series Integrated Services Routers	

		Cisco Aironet 2800 Series Access Points	
		Cisco Aironet 3500 Series running Cisco IOS Software	
		Cisco Aironet 3600 Series running Cisco IOS Software	
		Cisco Aironet 3700 Series running Cisco IOS Software	
		Cisco Aironet 3800 Series Access Points	
		Cisco Aironet 700 Series running Cisco IOS Software	
		Cisco Aironet AP801 Access Point running Cisco IOS Software	
		Cisco Aironet AP802 Access Point running Cisco IOS Software	
		Cisco Aironet AP803 Access Point running Cisco IOS Software	
		Cisco Aironet Access Points running Cisco IOS Software	
		Cisco Industrial Wireless 3700 Series running Cisco IOS Software	
		Cisco Meraki MR11	
		Cisco Meraki MR12	
		Cisco Meraki MR14	
		Cisco Meraki MR16	
		Cisco Meraki MR18	
		Cisco Meraki MR24	
		Cisco Meraki MR26	
		Cisco Meraki MR30HCisco Meraki MR32	
		Cisco Meraki MR33Cisco Meraki MR34	
		Cisco Meraki MR42	

		Cisco Meraki MR52	
		Cisco Meraki MR53	
		Cisco Meraki MR58	
		Cisco Meraki MR62	
		Cisco Meraki MR66	
		Cisco Meraki MR72	
		Cisco Meraki MR74Cisco Meraki MR84	
		Cisco Mobility Express	
		Cisco WAP121 Wireless-N Access Point with Single Point Setup	
		Cisco WAP321 Wireless-N Access Point with Single Point Setup	
		Cisco WAP371 Wireless-AC N Access Point with Single Point Setup	
		Cisco WAP551 Wireless-N Single Radio Selectable Band Access Point	
		Cisco WAP561 Wireless-N Dual Radio Selectable Band Access Point	
Espressif Systems	芯片模块	ESP8266	http://www.espressif.com/en/media_overview/news/espressif-releases-patches-wifi-vulnerabilities-cert-vu228519?position=0&list=nYFarqwM8ge2GgbOKKJ7XtnYePpzGN7rv1LOFEUlR3I
	软件	ESP32 ESP-IDF released versions v1.0, v2.0 and v2.1	
Fortinet .Inc	设备	FortiAP 5.6.1 以下（不含）	http://docs.fortinet.com/uploaded/files/3961/fortiap-v5.6.1-release-notes.pdf

FreeBSD Project			暂无
Google			暂无
Intel Corporation	设备	Intel® Dual Band Wireless-AC 3160	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00101&languageid=en-fr
	设备	Intel® Dual Band Wireless-AC 3165	
	设备	Intel® Dual Band Wireless-AC 3168	
	设备	Intel® Dual Band Wireless-AC 7260	
	设备	Intel® Dual Band Wireless-AC 7265	
	设备	Intel® Dual Band Wireless-AC 8260/8265/9260	
	设备	Intel Atom® Processor C3200 Series for Yocto Project BSP	
	软件	Intel® Active Management Technology	
Juniper Networks	platforms	SRX 210, 240 series firewalls with AX411 Wireless Access Points/Junos OS 12.1X46	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10827&actp=MEATDATA
	platforms	ScreenOS SSG-5 and SSG-20 devices with embedded Wireless Access Points radios/ScreenOS 6.3	
	platforms	MSS/WLAN 9.2, 9.6	
Mirochip Technology	芯片模块	WINC15x0 Family	http://www.microchip.com/design-centers/wireless-connectivity/embedded-wi-fi/wpa2-protocol-vulnerability
	芯片模块	RN171 / RN131	
	芯片模块	RN1810	
	芯片模块	WILC1000 / WILC3000 Linux	
Microsoft Corporatio	软件	Windows Server 2008 for 32-bit Systems Service Pack 2	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080

n	软件	Windows Server 2008 R2 for x64-based Systems Service Pack 1	
	软件	Windows Server 2012 R2 (Server Core installation)	
	软件	Windows 10 Version 1511 for 32-bit Systems	
	软件	Windows Server 2008 for x64-based Systems Service Pack 2	
	软件	Windows 8.1 for 32-bit systems	
	软件	Windows 8.1 for x64-based systems	
	软件	Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	
	软件	Windows Server 2012	
	软件	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	
	软件	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	
	软件	Windows 10 Version 1511 for x64-based Systems	
	软件	Windows 10 Version 1607 for x64-based Systems	
	软件	Windows 10 Version 1607 for 32-bit Systems	
	软件	Windows 7 for x64-based Systems Service Pack 1	
	软件	Windows 10 for x64-based Systems	
	软件	Windows Server 2012 (Server Core installation)	
	软件	Windows 7 for 32-bit Systems Service Pack 1	
	软件	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	
	软件	Windows Server 2012 R2	

	软件	Windows 10 for 32-bit Systems	
	软件	Windows RT 8.1	
	软件	Windows Server 2016	
	软件	Windows Server 2016 (Server Core installation)	
	软件	Windows 10 Version 1703 for x64-based Systems	
	软件	Windows 10 Version 1703 for 32-bit Systems	
OpenBSD			暂无
Peplink	产品	MAX: 700, OTG, BR1, BR1 Mini, BR1 Slim, BR1 Pro, HD2, HD2 IP67, HD4, Hotspot, Transit	https://forum.peplink.com/t/security-advisory-krack-wpa2-vulnerability-vu-228519/12715
	产品	MediaFast: HD2, HD4	
	产品	Surf: SOHO, On-The-Go	
	产品	Device Connector series	
Red Hat, Inc.	软件	Red Hat Enterprise Linux 6 (wpa_supplicant)	https://access.redhat.com/security/cve/cve-2017-15087
	软件	Red Hat Enterprise Linux 7 (wpa_supplicant)	
Sumsung Mobile			暂无
Sierra Wireless	设备	所有 Wi-Fi enabled 设备	https://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---wpa-and-wpa2-vulnerabilities/
Toshiba Commerce Solutions			补丁链接不可访问

Toshiba Electric Devices & Storage Corpation	固态硬盘	东芝 Canvio™ AeroMobile 无线固态硬盘	http://www.toshiba-personalstorage.cn/news/20171017.html
	无线硬盘	Canvio™ AeroCast / Canvio™ AeroCast 无线硬盘 HDTU110*KWC1*	http://www.toshiba-personalstorage.cn/news/20171018.html
Toshiba Memeory	设备	FlashAir™ W-04 无线局域网嵌入式 SDHC/SDXC 存储卡 THN-NW04W0640C6	http://www.toshiba-personalstorage.cn/news/20171017_1.html
	设备	FlashAir™ W-04 无线局域网嵌入式 SDHC/SDXC 存储卡 THN-NW04W0320C6	
	设备	FlashAir™ W-04 无线局域网嵌入式 SDHC/SDXC 存储卡 THN-NW04W0160C6	
Ubiauiti Networks	设备	Rocket 5AC Lite, model: R5AC-Lite	https://community.ubnt.com/t5/airMAX-Updates-Blog/airOS-v8-4-2-Has-Been-Released/ba-p/2101724
	设备	Rocket 5AC PTP AirPrism, model: R5AC-PTP	原通知有误
	设备	Rocket 5AC Multi-Point AirPrism, model: R5AC-PTMP	
	设备	PowerBeam 5AC, models: PBE-5AC-500, PBE-5AC-620, PBE-5AC-300, PBE-5AC-400	
	设备	PowerBeam 5AC 300 ISO, model: PBE-5AC-300-ISO	
	设备	PowerBeam 5AC 400 ISO, model: PBE-5AC-400-ISO	
	设备	PowerBeam 5AC 500 ISO, model: PBE-5AC-500-ISO	
	设备	NanoBeam 5AC 19dBi, model: NBE-5AC-19	
	设备	NanoBeam 5AC 16dBi, model: NBE-5AC-16	
	设备	LiteBeam 5AC 23dBi, model: LBE-5AC-23	
	设备	LiteBeam AC 16 dBi 120 degrees, model: LBE-AC-16-120	
	设备	Rocket 5AC Prism, model: R5-AC-PRISM	

	设备	PrismStation 5AC, model: PS-5AC	
	设备	IsoStation 5AC, model: IS-5AC	
	设备	NanoStation 5AC loco, model: NS-5ACL	
	设备	NanoBeam 5AC GEN2, model: NBE-5AC-GEN2	
	设备	LiteBeam 5AC GEN2, model: LBE-5AC-GEN2	
	设备	PowerBeam 5AC GEN2, model: PBE-5AC-GEN2	
	设备	Rocket Prism 5AC GEN2, model: RP-5AC-GEN2	
	设备	Bullet M2/M5/Titanium	https://community.ubnt.com/t5/airMAX-Updates-Blog/airOS-v6-1-2-Has-Been-Released/ba-p/2101714
	设备	Rocket M2/M2 Titanium/M3/M365/M900/M5/M5 GPS/M5 Titanium/M6	
	设备	NanoStation M2/M3/M365/M5/M6	
	设备	NanoStation Loco M2/M900/M5	
	设备	NanoBridge M2/M3/M365/M900/M5	
	设备	AirGrid M2/M5/HP/HP New	
	设备	PowerBridge M3/M365/M5/M10	
	设备	PicoStation M2	
	设备	AirRouter/HP	
	设备	PowerAP N	
	设备	LiteBeam M5	
	设备	NanoBeam M2/M5	
	设备	AirGrid M5 HP	
	设备	NanoStation M5	
	设备	NanoStation M5 Loco	

	设备	Rocket M5/Titanium	
	设备	UAP-AC-Lite/LR/Pro/EDU/M/M-PRO/IW/IW-Pro	https://community.ubnt.com/t5/UniFi-Updates-Blog/FIRMWARE-3-9-3-7537-for-UAP-USW-has-been-released/ba-p/2099365
	设备	UAP-AC-HD/SHD	
	设备	UAP, UAP-LR, UAP-OD, UAP-OD5	
	设备	UAP-v2, UAP-LR-v2	
	设备	UAP-IW	
	设备	UAP-Pro	
	设备	UAP-OD+	
	设备	USW	
	设备	US-L2-POE	
	设备	US-16-XG	
Ubuntu	软件	Ubuntu 17.04	https://usn.ubuntu.com/usn/usn-3455-1/
	软件	Ubuntu 16.04 LTS	
	软件	Ubuntu 14.04 LTS	
Watchguard Technologies, Inc.	设备	Access Points: AP100, AP102, AP120, AP200, AP300, AP320, AP322, AP420	https://www.watchguard.com/wgrd-blog/wpa-and-wpa2-vulnerabilities-update
	设备	Appliances: XTM 25-W, 26-W, 33-W; Firebox T10-W, T30-W, T50-W	
ZyXel	设备	NWA1100-NH	https://www.zyxel.com/support/announcement_wpa2_key_management.shtml
	设备	WAP6405	
	设备	WAP6804	
	设备	WAP6806	

	设备	WRE2206	
	设备	WRE6505 v2	
	设备	WRE6606	
	设备	Cam3115	
	设备	NWA5301-NJ	
	设备	NWA5123-AC	
	设备	WAC6103D-I	
	设备	WAC6500 series	