BREAKING NEWS

FOR IMMEDIATE RELEASE

Hackers Mobilize to Attack Routers

Competition scheduled to hack popular routers
in an effort to urge manufacturers to better protect consumers.

June 23, 2014

LAS VEGAS – An elite competition is scheduled for hackers and computer scientists from around the world to better protect consumers against widespread security vulnerabilities in wireless routers. A series of studies[1] in 2013 discovered a security epidemic affecting small office/home office (SOHO) wifi routers, wherein vulnerabilities allow an attacker to take control of the device and thereby intercept and modify network traffic. Abundant news coverage over the past 15 months has extensively reported the malicious exploitation of these devices, yet the epidemic persists today with little progress made by router manufacturers to address the issues. By bringing together the brightest minds in security, the hacking competition, dubbed "SOHOpelessly Broken" after the seminal research of the same title, seeks to identify new and existing security vulnerabilities in these widely deployed devices. "By demonstrating that the issues persist and that consumers are still exposed, pressure will be applied to the manufacturers to take the necessary action to better protect their customers who are currently not empowered to protect themselves," says Steve Bono, founder of ISE and one of the leaders of the event.

The competition will run during the renowned DEFCON hacker conference, from 7-10 August 2014 at the Rio Hotel & Casino in Las Vegas, NV. The contest will host a range of activities, including multiple talk tracks, Capture the Flag, 0-day vulnerability discovery, and others. The contest is organized by a partnership between two leading entities in the security community: Independent Security Evaluators (ISE) and the Electronic Frontier Foundation (EFF). ISE is the respected cyber security company most commonly known for being first to hack the iPhone and most recently for discovering the epidemic of security vulnerabilities in routers. The EFF is the leading nonprofit organization defending civil liberties in the digital world. DEFCON is one of the largest and oldest annual hacker conferences.

"The outcome of this event will be two-fold," says Ranga Krishnan of the EFF, "First, we will prove that routers are still vulnerable. Second, we will galvanize a community of technologists to demand remediation by manufacturers." EFF is also driving a related initiative known as the Open Wireless Movement (https://openwireless.org). In order to support this initiative, the EFF is developing a router on which users can confidently turn on an open WiFi channel that provides private internet access to guest users, without compromising the users' own security, privacy or internet experience.

Individuals interested in participating as contestants or as judges are encouraged to contact contest organizers as soon as possible through the contest website, www.sohopelesslybroken.com. Available spots are limited. Sponsorship and advertising opportunities are also available. The official hashtag of the event is *#sohopelesslybroken*.

About ISE
Founded in 2005 out of the PhD program at the Johns Hopkins' Information Security Institute, ISE is a sophisticated security consulting firm dedicated to aggressive defense strategies through advanced science. This select team of hackers, computer scientists, reverse engineers, and cryptographers utilizes a unique perspective typically perpetrated by the adversary. ISE is most commonly recognized for being the first company to exploit the iPhone[2], an achievement that garnered international attention. Other high profile compromises include ExxonMobil SpeedPass, Texas Instruments RFID, Diebold eVoting Machines, and numerous others. ISE's most recent research discovered systemic issues in SOHO routers[3] and web browsers[4].

[1] http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp
[2] http://www.nytimes.com/2007/07/23/technology/23iphone.html?_r=2&
[3] http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp
[4] http://securityevaluators.com/content/case-studies/caching/index.jsp

Contact:
Ted Harrington
Executive Partner
+1-443-270-2296
Ted.Harrington@securityevaluators.com

Independent Security Evaluators
4901 Springarden Drive, #200
Baltimore, MD 21217 USA
www.securityevaluators.com

About EFF
The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

Contact:
Ranga Krishnan
Technology Fellow
+1-415-436-9333
ranga@eff.org

Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
www.eff.org

About DEFCON
Started in 1993, DEFCON is one of the largest and oldest annual hacker conferences. DEFCON boasts a wide range of activities, including speeches, capture the flag, contests, lock picking, and official music events.

Contact:
Darrington Ford
Press Staffer
press@defcon.org

DEFCON
2606 2nd Ave
Seattle, WA 98101
www.defcon.org

Resources

- Groundbreaking ISE research discovers security vulnerability epidemic in routers: http://securityevaluators.com/knowledge/case_studies/routers/soho_router_hacks.php
- CNET first breaks story: http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/
- Open Wireless Movement: https://openwireless.org
- WIRED article about Open Wireless: http://www.wired.com/2014/06/eff-open-wireless-router/

Relevant routers news:

- NSA tampers with routers: http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden?r
- Routers are leverage points for attacks: http://nominum.com/news-post/24m-home-routers-expose-ddos/
- Routers used to hack bank accounts: http://thehackernews.com/2014/02/hackers-exploiting-router.html and http://www.scmagazine.com/vulnerabilities-in-home-routers-used-for-compromising-bank-accounts/article/333963/
- Mass exploit of top router manufacturer: https://isc.sans.edu/diary/Suspected+Mass+Exploit+Against+Linksys+E1000++E1200+Routers/17621
- Worm spreads attack from router to router: https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633
- Hackers take control of 300,000 home routers: http://news.techworld.com/security/3505049/criminals-hack-300000-home-routers-as-part-of-mystery-pharming-attack/
- Routers used to steal medical info: http://www.medicalpracticeinsider.com/best-practices/why-your-wi-fi-network-not-secure-you-think

~MORE~

Press

Press coverage of ISE routers research has been widespread. However, nothing has changed. Yet.
http://news.cnet.com/8301-1009_3-57579981-83/top-wi-fi-routers-easy-to-hack-says-study/

http://news.cnet.com/1606-2_3-50145624.html

http://www.forbes.com/sites/markgibbs/2013/04/20/2013-the-year-you-get-hacked/

http://dev.metro.msn-int.com/videohubpage?videoid=f4155dfb-fe5b-4892-b550-a1282dca0474&ap=True&refvid=05e2c935-dc72-4950-98b8-17e66cb04f11

http://www.pcworld.com/article/2035660/popular-home-routers-contain-critical-security-vulnerabilities.html

http://it.slashdot.org/story/13/04/17/2228258/researchers-hack-over-a-dozen-home-routers

http://www.computerworld.com/s/article/9238474/Popular_home_routers_contain_critical_security_vulnerabilities

http://article.wn.com/view-mobile/2013/04/17/Top_WiFi_routers_easy_to_hack_says_study/

http://www.ubergizmo.com/2013/04/your-off-the-shelf-wi-fi-router-can-easily-be-hacked/

http://news.techeye.net/security/wi-fi-routers-easy-to-crack

http://www.gizmoenvy.com/tag/independent-security-evaluators/

http://news.softpedia.com/news/Critical-Vulnerabilities-Found-in-13-SOHO-Routers-Many-Can-Be-Exploited-Remotely-346536.shtml

http://infosec42.blogspot.com/2013/04/exploiting-soho-routers.html

http://www.net-security.org/secworld.php?id=14776

http://www.infosecurity-magazine.com/view/31923/many-soho-routers-vulnerable

http://www.onlinegadgetstore.com/2299-wifi-routers-easy-access-hackers/

http://www.esecurityplanet.com/network-security/critical-security-flaws-found-in-home-office-routers.html

http://www.digitaltrends.com/computing/wi-fi-routers-hack/

http://www.technewsdaily.com/17797-many-popular-routers-can-easily-be-hacked.html

http://www.tgdaily.com/hardware-brief/71038-wi-fi-routers-are-easy-to-break-into

http://www.networkworld.com/news/2013/041813-popular-home-routers-contain-critical-268847.html

http://www.infopackets.com/news/security/2013/20130422_many_home_routers_vulnerable_to_attack_report.htm

http://checkthelog.wordpress.com/tag/independent-security-evaluators/

http://www.h-online.com/security/news/item/Groundhog-day-for-routers-1847381.html

http://dietrolldie.com/2013/04/19/two-birds-one-post-motion-to-quash-prenda-subpoena-wireless-firewallrouter-vulnerabilities/

http://www.metacafe.com/watch/cb-JXnjxme8yT40/inside_scoop_wi_fi_routers_susceptible_to_hacking/

http://www.hispanicbusiness.com/2013/9/16/remote_working_and_social_media_habits.htm

http://seclists.org/fulldisclosure/2013/Oct/282?utm_source=twitterfeed&utm_medium=twitter

http://www.medicalpracticeinsider.com/best-practices/why-your-wi-fi-network-not-secure-you-think

http://news.techworld.com/security/3505049/criminals-hack-300000-home-routers-as-part-of-mystery-pharming-attack/

END
###