PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

DA 17-799
Released: August 24, 2017

FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ENCOURAGES IMPLEMENTATION OF CSRIC SIGNALING SYSTEM 7 SECURITY BEST PRACTICES

The Federal Communications Commission's Public Safety and Homeland Security Bureau (Bureau) encourages communications service providers to implement the security countermeasures recommended by the Communications Security, Reliability, and Interoperability Council (CSRIC), a federal advisory committee to the FCC,[1] to prevent exploitation of carrier Signaling System 7 (SS7) network infrastructure.[2]

SS7 communications plays a critical role in U.S. commercial communications infrastructure. SS7 supports fixed and mobile service providers in processing and routing calls and text messages between networks, enabling fixed and mobile networks to connect, and providing call session information such as Caller ID and billing data for circuit switched infrastructure. Over the last several years, numerous research findings and media reports call attention to security vulnerabilities present within SS7 networks.[3] Reports suggest that attackers target SS7 to obtain subscriber information, eavesdrop on subscriber traffic, conduct financial theft, and promulgate denial-of-service attacks (DoS).[4]

---

[1] FCC, Communications Security, Reliability, and Interoperability Council V, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability#block-menu-block-4 (last visited July 20, 2017).

[2] Signaling System 7 (SS7) is a signaling protocol that supports call setup, routing, exchange, and billing functions in communications networks by transmitting messages between fixed and mobile service providers. CSRIC is a federal advisory committee composed of leaders from the private sector, academia, engineering, consumer/community/non-profit organizations, and government partners from tribal, state, local and federal agencies. *See* FCC Encyclopedia, Communications Security, Reliability and Interoperability Council III, http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii.

[3] *See* Sonus, Signaling System #7 Vulnerabilities: A Solution to Address SS7 Security Exposures (2016), https://www.sonus.net/sites/default/files/signalsystemvulnerabilities_may_2016.pdf.

[4] Matthew Braga, *Inside SS7, the Insecure Global Cell Network That's Used to Track Phones*, Motherboard (Aug. 27, 2014), https://motherboard.vice.com/en_us/article/inside-ss7-the-insecure-global-cell-network-thats-used-to-track-phones (explaining how SS7 data can be used to reveal location data); 60 Minutes: Hacking Your Phone (CBS television broadcast Apr. 17, 2016), http://www.cbsnews.com/news/60-minutes-hacking-your-phone/ (showing how SS7 may be used to eavesdrop on subscriber phone calls); Iain Thomson, *After Years of Warnings, Mobile Network Hackers Exploit SS7 Flaws to Drain Bank Accounts*, The Register (May 3, 2017), https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/ (revealing that SS7 exploits have allowed thieves to empty consumer bank accounts); Positive Research, *Attacking SS7: Mobile Operators Security Analysis*, PT Security (Aug. 31, 2016), http://blog.ptsecurity.com/2016/08/attacking-ss7-mobile-operators-security.html (revealing that SS7 exploits can be used to conduct DoS attacks against network subscribers).

In March 2017, CSRIC adopted recommendations for best practices to reduce SS7 security risks.[5] These recommendations can be grouped into the following two areas:

1) **Awareness and Protection:** This area covers the set of industry recommendations that advocate increased awareness of SS7 signaling and protective measures that can be deployed by telecommunication service providers. The four recommendations in this area are shown below:

    a) **Signaling Security Monitoring and Filtering:** Because communications service providers have "peer" relationships with each other, it is important to monitor the network interconnections used to pass traffic to and from networks.[6]

    b) **Aggregators:** Signaling aggregators can see network traffic originating from domestic and international entities. This provides active monitoring and filtering of network traffic to point and respond to suspicious traffic and minimize security risks.[7]

    c) **Ongoing Security Assessment of Signaling Infrastructure:** Robust security for SS7 network is critical to reducing security risks for current and emerging networks. Periodic security assessments of carrier SS7 infrastructure can identify security risks and provide security controls as needed.[8]

    d) **Subscriber Encryption Support:** Telecommunications service providers should educate consumers on applications providing end-to-end encryption services for voice calls.[9]

    e) **Threat Information Sharing:** Industry should continue its efforts in sharing threat information related to SS7 security risks with "the DHS National Coordinating Center for Communications (NCC), the Communications ISAC and collaboration with law enforcement."[10]

    f) **Automated Information Sharing Pilot:** Industry should continue working to develop use-case scenarios specific to SS7 security risks and incorporating those use-cases into the Automated Information Sharing (AIS) pilot program.[11]

2) **Security Best Practices:** This area covers the set of industry recommendations that deal with best security best practices for SS7 communications. In the case of Diameter, a next generation protocol supporting the same authentication, authorization, and accounting functions as SS7, CSRIC has also recommended awareness of related next generation protocols that will interact with SS7 infrastructures.

---

[5] *See* CSRIC V: Working Group 10, Legacy Risk Reductions (2017) (Legacy Risk Reductions Report), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

[6] *Id*. at 11 and 18.

[7] *Id*. at 13 and 18.

[8] *Id*. at 16 and 19.

[9] *Id*. at 15 and 19.

[10] *Id*. at 14 and 18.

[11] *Id*. at 14 and 18.

a) **GSMA Security Best Practices and Guidelines:** Industry should adhere to the SS7 security best practices delivered by the GSM Association (GSMA). The best practices include guidelines on increasing secure signaling and information sharing efforts.[12]

b) **Circles of Trust:** The Circles of Trust concept involves protecting and growing trust between service providers so they can safely pass traffic between networks. Industry should continue studying how Circles of Trust could benefit networks and their customers.[13]

c) **Diameter and 5G Networks:** Diameter supports the same functions as SS7 but may also introduce new vulnerabilities, which should be taken into account as 5G networks are deployed. Diameter is threatened by the same attack vectors as SS7 including traffic interception, fraud, and DoS attacks. Industry should continue to work with standards forums and other industry groups and follow security best practices endorsed by GSMA to "address emerging Diameter security risks."[14]

The Bureau recommends that communications service providers review the SS7 security best practices recommended by CSRIC to assess whether and how they may adapt or incorporate them into their own networks. Implementation of these mitigation solutions will benefit the commercial communications infrastructure and its end users by reducing SS7 security risks. Nearly all of the above topics are aimed at efforts that can commence now or in the near future. The exception is Diameter, which is a topic that is a subject for consideration by the current CSRIC.

For further information, contact Steven McKinnon, Engineer, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0390, steven.mckinnon@fcc.gov or Robert Finley, Attorney, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-7835, robert.finley@fcc.gov.

[12] *Id*. at 11 and 18.

[13] Legacy Risk Reductions Report, *supra* note 5 at 14-15 and 18.

[14] *Id*. at 12-13 and 18-19. *See* CSRIC VI Working Group Descriptions (2017), *available at* https://www.fcc.gov/files/csric6wgdescriptions6-2017pdf.