PUBLIC NOTICE

Federal Communications Commission
45 L St., N.E.
Washington, D.C. 20002

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

DA 24-308
Released: March 27, 2024

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REQUESTS COMMENT ON IMPLEMENTATION OF MEASURES TO PREVENT LOCATION TRACKING VIA THE DIAMETER AND SIGNALING SYSTEM 7 SECURITY PROTOCOLS

PS Docket No. 18-99

Comments Due: April 26, 2024
Reply Comments Due: May 28, 2024

The Federal Communications Commission's Public Safety and Homeland Security Bureau (Bureau) requests comment on communications service providers' implementation of security countermeasures to prevent exploitation of vulnerabilities in the Signaling System 7 (SS7) and Diameter protocols to track the location of consumers through their mobile devices.

Background:

The Signaling System 7 (SS7) and Diameter protocols play a critical role in U.S. telecommunications infrastructure supporting fixed and mobile service providers in processing and routing calls and text messages between networks, enabling interconnection between fixed and mobile networks, and providing call session information such as Caller ID and billing data for circuit switched infrastructure. Over the last several years, numerous reports have called attention to security vulnerabilities present within SS7 networks and suggest that attackers target SS7 to obtain subscribers' location information.[1]

The Diameter protocol provides the same services as SS7 and as a result presents similar vulnerabilities. The Diameter protocol was originally used as the standard signaling protocol intended for exchanging authentication, authorization, and accounting information in fixed and mobile networks. Diameter was expanded to include support for network access and IP mobility in local and roaming

[1] *See, e.g.*, 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 track location); 60 Minutes: Hacking Your Phone (CBS television broadcast Apr. 17, 2016), http://www.cbsnews.com/news/60-minutes-hacking-your-phone/ (demonstrating how SS7 may be used to track a subscriber); Sean Lyngaas, *DHS: 'Nefarious actors' Could Be Exploiting SS7 Flaw,* CyberScoop (Jun. 1, 2018), https://cyberscoop.com/ss7-stingrays-imsi-catchers-chris-krebs-dhs-ron-wyden/ (describing how IMSI catchers exploit SS7 vulnerabilities to imitate a cell tower to intercept caller location).

situations.[2] Diameter does not encrypt originating IP addresses during transport, which increases the risk of network spoofing, where an attacker poses as a legitimate roaming partner on a network to gain access to the network.[3] While technology is evolving, the SS7 and Diameter protocols are still the foundation for mobile telephone networks, especially for roaming capabilities to be able to interconnect networks. As coverage expands, and more networks and participants are introduced, the opportunity for a bad actor to exploit SS7 and Diameter has increased.[4]

In response to these threats, the Communications Security, Reliability, and Interoperability Council (CSRIC), a federal advisory committee to the FCC, established working groups to assess the security risks associated with the SS7 and Diameter protocols and develop recommendations to mitigate those risks accordingly.[5] In June 2016, CSRIC V Working Group 10, "Legacy Systems and Services Risk Reduction," began studying these problems and in March 2017, CSRIC V adopted a final report detailing the vulnerabilities in the SS7 and Diameter protocols and provided specific recommendations for best practices to help prevent exploitation of SS7.[6] These recommendations included the use of firewalls, monitoring, and filtering to reduce the ability of an attacker to gain access to subscribers' location and engaging with signaling aggregators, which provide a "wider view of signaling traffic originating from domestic and international entities and terminating in the U.S. telecommunications network."[7] The recommendations also included the importance of security assessments and threat information sharing in order to detect incidents of location tracking and increase situational awareness of providers.[8] CSRIC V also recommended that industry encourage subscribers to use available encryption technologies in order to reduce access by a bad actor.[9] CSRIC V additionally recommended continuing to examine and address the security practices related to next generation protocols, including Diameter.[10]

In 2018, CSRIC VI identified location tracking as one of the primary motivations behind potential attacks in SS7 and Diameter.[11] CSRIC VI noted:

> "Location tracking in the SS7/Diameter sense does not provide granular location data for a consumer. The information retrieved through location tracking is therefore limited to cell ID or serving MSC/MSS address, which in itself may disclose the city or general area within a city for a target, but not specific GPS coordinates as seen with other attack

[2] Communications Security, Reliability and Interoperability Council VI: Working Group 3 Network Reliability and Security Risk Reduction, *Recommendations to Mitigate Security Risks for Diameter Networks* at 11 (2018), https://www.fcc.gov/sites/default/files/csric6report_recommendationstomitigateriskdiamterprotocol032018.pdf (CSRIC VI Report).

[3] *Id.* at 29.

[4] *Id.* at 13.

[5] CSRIC is an advisory committee of the Federal Communications Commission, the mission of which is to make recommendations to the Commission to promote the security, reliability and resiliency of the Nation's communications systems. FCC, Communications Security, Reliability, and Interoperability Council (CSRIC), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 .

[6] Communications Security, Reliability and Interoperability Council V: Working Group 10, Legacy Systems Risk Reductions (2017), https://www.fcc.gov/sites/default/files/CSRIC5-WG10-FinalReport031517.pdf (CSRIC V Report).

[7] *Id.* at 11, 13, 18-19.

[8] CSRIC V Report at 18-19.

[9] *Id.* at 19.

[10] *Id.*

[11] CSRIC VI Report at 26.

> vectors (such as malware on a device where these coordinates can be retrieved). Even this information can be harmful though, depending on the subscriber. VIPs and government officials need to be especially wary of this possibility. . . . Location tracking is the process of attaining individualized information of subscribers' locations to develop pattern maps of the target's whereabouts. . . . If the cell ID and/or location codes are revealed, the attacker has the ability to determine the location of the cell tower through publicly available websites. . . . There are several other ways for retrieving [cell tower or visited network] information, so not every attack is the same. Attackers will use a variety of methods depending on the response received from the network they are attacking."[12]

CSRIC VI also issued recommendations concerning best practices to reduce exploitation of the Diameter protocol which were similar to the SS7 recommendations, and made additional recommendations concerning network administration.[13] This recommendation advised that network administrators implement secure domains and that security gateways, which interconnect the domains, be deployed at network boundaries to reduce unauthorized access.[14]

The Commission has encouraged communications service providers to implement the security countermeasures developed and recommended by CSRIC.[15] In April 2018, the Commission released a Public Notice requesting comment on the progress and effectiveness surrounding the implementation of SS7 protocol security best practices.[16] Commenters included larger communications service providers who described that they have implemented the CSRIC recommendations and other best practices relevant to their networks.[17] In February 2020, the Commission released an additional Public Notice requesting comment on the progress and effectiveness surrounding the implementation of Diameter protocol security

[12] *Id.* at 27.

[13] *Id.* at 37-38 (recommending the use of message filtering and evaluation of Diameter peer relationships, GSMA security best practices to secure signaling interconnections, threat information sharing, security assessments, and subscriber media encryption support and user authentication).

[14] *Id.* at 38.

[15] In August 2017, the Commission released a Public Notice recommending that communications service providers implement the CSRIC V Working Group 10 SS7 best practices. *See FCC's Public Safety and Homeland Security Bureau Encourages Implementation of CSRIC Signaling System 7 Security Best Practices*, DA 17-799, Public Notice (PSHSB Aug. 24, 2017).

[16] *Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Best Practices*, DA 18-333, Public Notice (PSHSB Apr. 3, 2018).

[17] *See* AT&T Services, Inc. Comments at 3-4 (rec. May 4, 2018) (describing that AT&T has implemented extensive blocking and filtering of malicious SS7 messages, SMS Home Routing, new firewalls and other technologies to monitor and filter traffic, advanced filtering as recommended by GSMA; tested its network to assess threats to its network and responded accordingly; and continued collaboration with the Commission and other agencies and industry to share threat information and responses); CTIA Comments at 7-9 (rec. May 3, 2018) (describing the implementation of CSRIC recommendations and GSMA best practices by various carriers); Sprint Corporation Comments at 4-6 (rec. May 3, 2018) (explaining the measures Sprint has taken to protect its SS7 network including the use of Code Division Multiple Access technology and implementing relevant GSMA best practices, and also noting the particular effectiveness of monitoring and filtering practices to reduce exploitation in SS7); T-Mobile USA, Inc. Comments at 4 (rec. May 3, 2018) (explaining that T-Mobile has implemented CSRIC V recommendations including a "SS7 special-purpose firewall" designed to enhance monitoring and filtering, updated its consumer education materials concerning encryption, and continuing to share threat information with government and industry); Verizon Comments at 1-3 (rec. May 3, 2018) (explaining Verizon has implemented the GSMA recommendations relevant to reduce vulnerabilities posed by other carriers when Verizon's customers roam on GSM networks and also implemented a signaling firewall, penetration testing, consumer education about encryption options, and threat information sharing, among other security measures);

best practices.[18] The same commenters described their implementation of the CSRIC recommendations and other best practices concerning the vulnerabilities of the Diameter protocol.[19] In July 2020, the Commission acknowledged the progress industry made in addressing Diameter security issues, noting the widespread adoption of CSRIC's recommendations across the industry.[20]

Most recently, in a February 2024 letter addressed to President Biden, Senator Ron Wyden outlined his continued concerns about the ability of foreign authoritarian governments to surveil and track the location of individuals by exploiting vulnerabilities in SS7 and Diameter, and called on the Commission to implement minimum cybersecurity requirements for wireless carriers, among other recommendations.[21]

Request for Comment:

To this point, the Bureau has broadly focused on providers' efforts to reduce or mitigate overall vulnerabilities in the SS7 and Diameter protocols. The Bureau finds it is important to more specifically examine the area of location tracking. To that end, the Bureau seeks renewed public comment, including from communications service providers and other stakeholders, on the implementation and effectiveness of security countermeasures, including but not limited to the CSRIC V and VI recommendations regarding the SS7 and Diameter protocols, with respect to location tracking, including any progress, barriers, and lessons learned, and the extent to which these recommendations are supported by providers. Where applicable, we ask that commenters provide information about how the questions and your answers apply to their own systems and services:

- **Incidents of Location Tracking:** Have there been any successful, unauthorized attempts to access the network user location data of communications service providers operating in the United States to track user location using exploits in the SS7 or Diameter protocols since CSRIC VI's adoption of best practices in 2018? If so, we ask that commenters provide the date(s) of the incident; a description of the location tracking that occurred; a description of the vulnerabilities exploited and the techniques used to access the system; and the identity of the attacker, if known. What actions, if any, have communications service providers taken in

[18] *Public Safety and Homeland Security Bureau Requests Comment on Implementation of Diameter Best Practices*, DA 20-141, Public Notice (PSHSB Feb. 10, 2020).

[19] *See* AT&T Services, Inc. Comments at 2-3 (rec. Mar. 11, 2020) (explaining AT&T's implementation of extensive blocking and filtering, participation in standards forums to develop global security standards, and sharing of threat information, among other best practices); CTIA Comments at 6-15 (rec. Mar. 11, 2020) (describing providers' implementation of various recommendations); Sprint Corporation Comments at 4-5 (rec. Mar. 11, 2020) (explaining that Sprint has implemented CSRIC recommendations including monitoring and message filtering practices); T-Mobile USA, Inc. Comments at 3-7 (rec. Mar. 11, 2020) (explaining that it has implemented the CSRIC recommendations and the GSMA best practices and guidelines for Diameter internetwork peering and securing its signaling interconnections, among other recommendations); Verizon Comments at 1-5 (rec. Mar. 11, 2020) (explaining how it has implemented each of the CSRIC recommendations).

[20] Press Release, Chairman Ajit Pai, FCC, Chairman Pai Announces Industry Progress in Addressing Diameter Network Security Issue (Jul. 27, 2020), https://www.fcc.gov/document/pai-announces-industry-progress-addressing-diameter-security-issue.

[21] Letter from Ron Wyden, U.S. Senator, to Joseph Biden, President of the United States (Feb. 29, 2024), https://www.wyden.senate.gov/imo/media/doc/wyden-phone-hacking-letter-to-president-biden.pdf (copying Chairwoman Rosenworcel and other federal agency officials). Senator Wyden has previously called attention to the vulnerabilities in SS7. In 2017, Senator Wyden and Representative Ted Lieu urged the Commission, in light of the CSRIC V report, to implement CSRIC's recommendations, and to continue examining the risks identified in the CSRIC V report through future CSRIC working groups. Letter from Ron Wyden, U.S. Senator, and Ted Lieu, U.S. Representative, to Ajit Pai, Chairman, FCC (Mar. 28, 2017); *see also* Letter from Ron Wyden, U.S. Senator to Ajit Pai, Chairman, FCC (May 29, 2018) (outlining the threats that SS7 vulnerabilities pose to national security and urging the Commission to take regulatory action over wireless carriers).

response to any unauthorized attempts to access the location repository? Were there any steps that communications service providers could have taken to prevent these incidents before they occurred?

The malicious use of global titles can potentially enable the tracking of phones both domestically and internationally.[22] Since CSRIC VI's adoption of best practices in 2018, have there been any incidents in which a leased United States global title was exploited to track the location of a customer in the United States? If so, we ask that commenters provide the date(s) of the incident; a description of the location tracking that occurred; a description of the vulnerabilities exploited and the techniques used to access the system; information on the ownership and leasing of any global titles involved in the incident; and the identity of the attacker, if known

- **Preventing Exploitation of Location Information:** We seek comment on the measures that communications service providers have implemented to protect the location tracking of their customers via the SS7 and Diameter protocols. Which CSRIC recommendations for SS7 or Diameter, or any other industry best practices including the GSMA best practices, concerning location tracking have communications service providers implemented? Have service providers implemented GSMA FS.19 "Diameter Security" requirements in their Authentication, Authorization, and Accounting (AAA) networks? What measures have providers implemented to prevent location information from being exploited by companies with which providers have roaming agreements? Are there specific measures that all providers should be implementing that are not addressed in existing best practices? What barriers have communications service providers encountered in implementing the recommendations? What factors have communications service providers used to determine whether any of the recommendations concerning location tracking are not suitable for their networks? Have smaller providers implemented measures to prevent location information from being exploited, and if not, why? How can the Commission have more visibility into the steps that providers of all sizes are taking to mitigate SS7 and Diameter vulnerabilities and more confidence that those steps are effective? For example, are providers currently conducting third-party audits of their SS7 and Diameter security measures? If so, should the results of those audits be reported to the Commission or other federal agencies?

[22] *See* GSMA, GSMA Global Title Leasing Code of Conduct, https://www.gsma.com/security/gtleasing/ (last visited on Mar. 19, 2024) ("A global title (GT) is an address used for routing signaling messages (using the Signalling (*sic*) Connection Control Part / SCCP protocol) on telecommunications networks. National authorities allocate numbering resources to communications providers, which reserve and use part of those numbers for use as GTs. In mobile networks, GTs enable information to be exchanged within and between networks, so that mobile services work regardless of whether a user is in his/her home network or roaming.").

- **Leasing of Global Titles:** What vulnerabilities have communications service providers observed related to the leasing, subleasing, or other arrangements involving the conveyance of global titles? Have communications service providers conveyed global titles to entities outside of the United States, and if so, to whom? When entering into an arrangement concerning the leasing, subleasing, or conveying or global titles, do these arrangements limit the third party's ability to further convey the global title or require the implementation of security measures to prevent unauthorized location tracking? What specific measures have been implemented to reduce security risks when leasing, subleasing, or conveying global titles? Are smaller communications service providers leasing, subleasing, or conveying global titles? How can the Commission have more visibility into the conveyance of global titles to ensure that they are not being exploited to obtain the location of subscribers in the United States? For example, should the Commission require the conveyance of global titles to be reported to the Commission?

Procedural Matters

Interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the FCC's Electronic Comment Filing System (ECFS).

- Commenting parties may file comments in response to this Notice in PS Docket No. 18-99.
- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701. U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, D.C., 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. *See FCC Announces* Closure *of FCC Headquarters Open Window and Change in Hand-Delivery Policy*, Public Notice, 35 FCC Rcd 2788 (OMD 2020), https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at (202) 418-0530 (voice), (202) 418-0432 (tty).

Parties wishing to file materials with a claim of confidentiality should follow the procedures set forth in Section 0.459 of the FCC's rules. Casual claims of confidentiality are not accepted. Confidential submissions may not be filed via ECFS but rather should be filed with the Secretary's Office following the procedures set forth in 47 CFR § 0.459. Redacted versions of confidential submissions may be filed via ECFS. Parties are advised that the FCC looks with disfavor on claims of confidentiality for entire documents. When a claim of confidentiality is made, a public, redacted version of the document should also be filed.

We exempt the proceeding initiated by this Notice from the FCC's *ex parte* rules.[23] This exemption serves the public interest by facilitating the full discussion of potentially sensitive matters. In

[23] 47 CFR § 1.1200(a).

the event the Commission were to take further action, any rule that the Commission were to propose would be subject to permit-but-disclose rulemaking procedures before it would be adopted, which would ensure the compilation of a full record.

For further information, contact Rebecca Clinton, Attorney Advisor, Operations and Emergency Management Division, Public Safety and Homeland Security Bureau, (202) 418-7815, rebecca.clinton@fcc.gov.

– FCC –