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 20-141
Released: February 10, 2020

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REQUESTS COMMENT ON IMPLEMENTATION OF DIAMETER PROTOCOL SECURITY BEST PRACTICES

Comment Date: March 11, 2020

In March 2018, the Federal Communications Commission's Communications Security, Reliability and Interoperability Council VI (CSRIC VI)[1] recommended that communications service providers implement certain security measures to mitigate network reliability and security risks associated with the Diameter protocol.[2] CSRIC VI provided eight recommendations for reducing Diameter security risks and increasing situational awareness. *See* Attachment. The Diameter protocol is a critical component of telecommunications infrastructure, used to exchange authentication, authorization, and accounting information in fixed and mobile networks.[3] While Diameter provides a more reliable, secure, and flexible framework for exchanging exchange authentication, authorization, and accounting messages than legacy protocols, it does introduce some vulnerability to the network. Diameter does not encrypt originating IP addresses during transport, a vulnerability that increases the risk of a malicious actor posing as a legitimate roaming partner on a network can gain access to the target network. Implementation of CSRIC VI's recommendations may help reduce these threats associated with the Diameter protocol.

The Bureau seeks public comment, including from communications service providers and other stakeholders, on the implementation and effectiveness of the CSRIC VI recommendations regarding the Diameter protocol, including any progress, barriers, and lessons learned. The Bureau also seeks comment on any alternatives to the CSRIC VI recommendations that communications service providers have implemented or plan to implement to help address Diameter protocol security risks. The Bureau is particularly interested in comment on the following sets of questions as they relate to the CSRIC VI recommendations. Where applicable, we ask that commenters provide information about how the questions and your answers apply to your own unique situation:

- **Progress:** What progress has been made by communications service providers in implementing the recommendations? To the extent communications service providers plan to implement the recommendations but have not yet done so, what are their plans to implement

---

[1] 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-interoperabilitycouncil-0 (last visited Jan. 16, 2020).

[2] *See* Communications Security, Reliability and Interoperability Council VI, *Recommendations to Mitigate Security Risks for Diameter Networks* (2018), https://www.fcc.gov/files/csric6wg3finalreport32018pdf, pp 37-38.

[3] These include Long-Term Evolution and IP Multimedia Systems networks, which use a framework for delivering IP multimedia services.

the recommendations? What are their reasons for postponing implementation? What factors have communications service providers considered in devising their implementation plans? 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 are not suitable for their networks?

- **Evaluation:** What successes, including in communications security risk reduction, have communications service providers realized by implementing the recommendations? What indicators (qualitative and quantitative) have communications service providers used to determine the correlation between implementation of the recommendations and reduction in Diameter security risks? How effective are the recommended measures in reducing Diameter security risks? Are there alternatives that could be more effective than the measures recommended by CSRIC, and if so, what are these alternatives and why are they more effective?

- **Other Considerations:** Have communications service providers shared potential Diameter security risks with their various internal business units and key business clients that rely on Diameter signaling as well as to interconnected peer providers, and if so, how? What measures have been implemented to help protect the privacy of subscriber data from Diameter exploits? How long do communications service providers keep Diameter network logs in the normal course of business, and would longer retention times be helpful in responding to potential Diameter security compromises?

Procedural Matters

Pursuant to Sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, 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). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 CFR 24121 (1998).

- 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: http://apps.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 hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the FCC's Secretary, Office of the Secretary, Federal Communications Commission.
- All hand-delivered or messenger-delivered paper filings for the FCC's Secretary must be delivered to FCC Headquarters at 445 12th Street, SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
- 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 445 12th Street, SW, Washington, DC 20554.

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.[4] This exemption serves the public interest by facilitating the full discussion of potentially sensitive matters. In 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 Suzon Cameron, Designated Federal Officer (DFO), CSRIC VII, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-1916, Suzon.Cameron@fcc.gov or Kurian Jacob, Deputy DFO, CSRIC VII, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-2040, Kurian.Jacob@fcc.gov.

-FCC-

[4] 47 CFR §§ 1.1200(a).

ATTACHMENT

CSRIC VI Recommendations to Mitigate Security Risks for
Diameter Networks

1) **US Critical Infrastructure Protection**
   Consistent with Cybersecurity Risk Management and Best Practices from CSRIC V and recommendations from subject matter experts, it is recommended that industry evaluate Diameter peer relationships based on the GSMA guidelines and recommended service level terms. Message filtering based on GSMA recommendations are viewed as having the most significant mitigating impact.

2) **GSMA Security Best Practices and Guidelines**
   The CSRIC recommends that industry use the GSMA security best practices and guidelines to secure signaling interconnections for Diameter as described in Section 4.

3) **Threat Information Sharing**
   The CSRIC recommends and endorses continuing efforts to improve information sharing of threat intelligence that can be used to adapt monitoring, filtering and data analytics, see Section 4.

4) **Diameter in Emerging 5G Networks**
   The CSRIC recommends that the industry continue to participate in industry and standards forums and adopt the GSMA recommended controls to address emerging security risks as part of their overall 5G and IoT security approach as outlined in Section 6 and 7.

5) **Subscriber Media Encryption Support and User Authentication**
   The CSRIC recommends that industry encourage the use of available media encryption technologies, for both voice and data communications, in particular for highly sensitive and critical applications or for Very Important Persons (VIPs) that may often be targeted by bad actors. Over the long-term CSRIC recommends continued tracking and assessment of advancements in end-to-end user authentication, media integrity protection and media encryption techniques.

6) **Security Assessments**
   The CSRIC recommends and endorses security assessments as a tool to be applied and used based on specific network architectures, CSRIC further recommends continued risk management based on the unique requirements of each network and the corresponding unique test results.

7) **Network Administration**
   CSRIC Recommends that Network Administrators implement secure domains, and if they serve multiple countries, each country should be operating in its own domain. Security domains are interconnected through security gateways (SEGs). Security gateways are deployed at the network boundaries to protect against attacks and unauthorized access. CSRIC Recommends that a security gateway is implemented with limited access to network resources, to limit attack surfaces. The security gateway is only used to protect the control plane and not the user plane.21

8) **North America Circle of Trust**
   For North America, consideration should be given to a Circle-of-Trust initiative. This initiative should include discussion of collaboration to help meet potential threats. All operators in the region must agree on this, and measures could be implemented to increase visibility to traffic in and out of those networks.