

June 2023

**Communications Security, Reliability, and Interoperability Council VIII**

**Report on**

**Best Practices to Mitigate Security Vulnerabilities in HTTP/2**

Drafted by

Working Group 1: 5G Signaling Protocols Security

Table of Contents

[1 Results in Brief 3](#_Toc134649852)

[1.1 Executive Summary 3](#_Toc134649853)

[2 Introduction 3](#_Toc134649854)

[2.1 CSRIC VIII Structure 4](#_Toc134649855)

[2.2 Working Group 1 Team Members 4](#_Toc134649856)

[3 References 5](#_Toc134649857)

[4 Objective, Scope, and Methodology 6](#_Toc134649858)

[4.1 Objective 6](#_Toc134649859)

[4.2 Scope 6](#_Toc134649860)

[4.3 Methodology 7](#_Toc134649861)

[4.4 Presentations from Subject Matter Experts 7](#_Toc134649862)

[5 Background and Related 5G Security Activities 8](#_Toc134649863)

[5.1 Use of HTTP/2 Protocols in 3GPP Systems 8](#_Toc134649864)

[5.2 3GPP Service Based Architecture (SBA) Overview 8](#_Toc134649865)

[5.3 3GPP Service Based Management Architecture Overview 9](#_Toc134649866)

[5.4 Standardization of HTTP and HTTPS in IETF 10](#_Toc134649867)

[5.5 HTTP/2 and HTTPS in 5G standards 11](#_Toc134649868)

[5.6 Non-Core Usage of HTTP (non-3GPP) 12](#_Toc134649869)

[6 Analysis of Protocol Vulnerabilities’ impact on 5G 12](#_Toc134649870)

[6.1 Analysis & Observations 12](#_Toc134649871)

[6.1.1 Client Initiated Attacks on Servers 12](#_Toc134649872)

[6.1.2 Heist Attack 15](#_Toc134649873)

[6.1.3 Custom HTTP/2 Headers 15](#_Toc134649874)

[6.1.4 Implementation Vulnerabilities 16](#_Toc134649875)

[6.2 Best Practices and Recommendations 16](#_Toc134649876)

[6.2.1 Client Initiated Attacks on Servers 17](#_Toc134649877)

[6.2.2 Heist Attack: Recommended Mitigation 20](#_Toc134649878)

[6.2.3 Custom HTTP/2 Headers Mitigation 20](#_Toc134649879)

[6.2.4 Implementation Vulnerabilities: Recommended Mitigation 20](#_Toc134649880)

[6.2.5 General Recommendations 21](#_Toc134649881)

[Appendix A: Enumerated Protocol Vulnerabilities 22](#_Toc134649882)

[Appendix B: Glossary of Acronyms 24](#_Toc134649883)

# Results in Brief

## Executive Summary

As described in the previous report, in 5G, the earlier architectures have been eliminated, and a new architecture built on IT and cloud technology has been defined in its place. In addition to a new architecture, the control plane signaling has been replaced with Hypertext Transfer Protocol Version 2 (HTTP/2) protocol being used with JavaScript Object Notation (JSON), based on existing IT technology.

This departure from traditional technology and architectures is necessary in order to deliver the ultra-high speeds and bandwidth needed to support use cases with video and other real-time applications. Low latency requirements also required a change in the architecture to support more computing at the edge and new processes for managing IoT. These requirements are designed to support the connectivity of billions of “things” in our world, for use cases such as smart cities, industrial automation, TeleHealth, and connected vehicles.

While very familiar to the IT sector, this new architecture is unlike anything the industry has dealt with before and introduces new attack vectors. One of those attack vectors is the HTTP/2 protocol being used with JSON for signaling in the 5G network.

It is important to note that while there may be many vulnerabilities identified in HTTP/2, these are all based on public access to the network (such as through the Internet) and not in a closed network as is the case with 5G. This was taken into consideration throughout our research.

CSRIC VIII Working Group 1 was tasked with identifying 5G signaling vulnerabilities associated with the HTTP/2 protocol specifically. The FCC asked CSRIC VIII, and delegated to Working Group 1, to first provide a report on what vulnerabilities existed in HTTP/2 relevant to 5G. That report was completed in September 2022.[[1]](#footnote-2) This second report provides recommendations on mitigation and best practices for those vulnerabilities identified in the earlier report.

# Introduction

In the previous report, CSRIC VIII Working Group 1 (WG1) examined known HTTP/2 protocol vulnerabilities based on existing sources, input from the FCC as well as presentations from subject matter experts. This report focuses on the analysis of the vulnerabilities and recommended risk mitigations as it relates to the security of the 5G control plane and its associated signaling and highlights key observations and conclusions. For ease of reference, this report leverages the same text from the prior report and adds-in the corresponding recommended risk mitigations.

The task of providing recommendations to prevent HTTP/2 vulnerabilities from being repeated in HTTP/3 has been deferred. The 3GPP standards efforts have not yet endorsed HTTP/3 for use in 5G networks (or any future networks for that matter). WG1 has deferred this research to future CSRICs once the 3GPP endorses use of HTTP/3 for use in signaling networks.

## CSRIC VIII Structure

CSRIC VIII was established at the direction of the Chairwoman of the FCC in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The purpose of CSRIC VIII is to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems. CSRIC VIII’s recommendations will focus on a range of public safety and homeland security-related communications matters. The FCC created informal subcommittees under CSRIC VIII, known as working groups, to address specific tasks. These working groups must report their activities and recommendations to the Council as a whole, and the Council may only report these recommendations, as modified or ratified, as a whole, to the Chairwoman of the FCC.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Communications Security, Reliability, and Interoperability Council (CSRIC) VIII** | | | | | |
| **CSRIC VIII Working Groups** | | | | | |
| Working Group 1: 5G Signaling Protocols Security | Working Group 2: Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment | Working Group 3: Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks | Working Group 4: 911 Service over Wi-Fi | Working Group 5: Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure | Working Group 6: Leveraging Mobile Device Applications and Firmware to Enhance Wireless Emergency Alerts |
| Co-Chairs:  Brian Daly, AT&T  Travis Russell, Oracle | Co-Chairs:  Mike Barnes, Mavenir  George Woodward, RWA | Co-Chairs:  Micaela Giuhat, Microsoft  John Roese, Dell | Co-Chairs:  Mary Boyd, Intrado  Mark Reddish, APCO | Co-Chairs:  Todd Gibson, T-Mobile  Padma Sudarsan, VMWare | Co-Chairs:  Farrokh Khatibi, Qualcomm  Francisco Sanchez, SBA |
| FCC Liaison:  Ahmed Lahjouji | FCC Liaison:  Zenji Nakazawa | FCC Liaison:  Jeff Goldthorp | FCC Liaison: Rasoul Safavian | FCC Liaison:  Zenji Nakazawa | FCC Liaison:  James Wiley,  Tara Shostek |

Table 1 - Working Group Structure

## Working Group 1 Team Members

Working Group 1 consists of the members listed below.

|  |  |
| --- | --- |
| **Name** | **Company** |
| Brian K. Daly\* (Co-Chair) | AT&T Services Inc. |
| Travis Russell\* (Co-Chair) | Oracle Communications |
| Matt Carothers | Cox Communications |
| Martin Goldberg\* | National Security Agency |
| Angel Gomez | Verizon Communications |
| Stephen Hayes\* | Ericsson |
| Jithin Jagannath | ANDRO Computational Solutions |
| Antwane Johnson\* | Federal Emergency Management Agency |
| Ahmed Lahjouji | FCC |
| Xiaoyang Lee | Cybersecurity and Infrastructure Security Agency |
| John Marinho | CTIA |
| Martin McGrath | Nokia |
| Maureen Mclaughlin\* | Satellite Industry Association |
| Danny McPherson\* | Verisign |
| Derek Peterson\* | Wireless Broadband Alliance |
| Mitch Rappard | Palo Alto Networks |
| Mike Recchione | Alliance for Telecommunications Industry Solutions |
| Christopher Wendt | Somos |
| Michael Bergman | Consumer Technology Association (CTA) |

Table 2 - List of Working Group Members

\* CSRIC Members

The Working Group members had an option to nominate an alternate to participate in the discussions when they were unavailable. Although these alternates are not a member of the Working Group and may not vote, they provided valuable input towards the completion of this report that should be acknowledged. Working Group 1 alternate members are listed in

Table 3.

|  |  |
| --- | --- |
| **Name** | **Company** |
| Adam Barron | Verizon Communications |
| Martin Dolly | AT&T Services Inc. |
| Carroll Gray-Preston | ATIS |
| Brandon Hinton | Satellite Industry Association |
| David Grossman | Consumer Technology Association (CTA) |
| Navin Jaffer | CISA |
| Young Kim | Verisign Inc. |
| John Mattson | Ericsson |
| Mark Lucero | FEMA |
| Bradley Jackson | Verizon Wireless |

Table 3 - List of Working Group Alternate Members

# References

1. The 3GPP defined Service Based Management Architecture White Paper (Nokia Bell Labs) See: [The 3GPP-defined Service Based Management Architecture (nokianews.net)](https://nokianews.net/files/Nokia_Bell_Labs_The_3GPP-defined_Service_Based_Management_Architecture_White_Paper_EN.pdf)
2. 3GPP 28.533 Management and orchestration; Architecture framework See: [Specification # 28.532 (3gpp.org)](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3427)

1. 3GPP TR 29.893 Study on IETF QUIC Transport for 5GC Service Based Interfaces
2. HTTP/2: In-depth analysis of the top four flaws of the next generation web protocol; Imperva, Hacker Intelligence Initiative; August 2016, V1
3. Signalling Security Analysis: Is HTTP/2 Secure in 5G Core Network?; Hu, Xinxin; Liu, Caixia; You, Wei; Zhao, Yu; National Digital Switching System Engineering & Technological Research Center; Zhengzhou China
4. HTTP/2: The Sequel is Always Worse; Kettle James
5. IETF RFC 9113; Hypertext Transfer Protocol Version 2 (HTTP/2); June 2022
6. 5G Network Slicing Security; McDaid, Cathal, AdaptiveMobile; Feb 2022
7. 3GPP TS 33.117 v17.0.0; Catalogue of general security assurance requirements
8. QUIC and HTTP/3; Ericsson presentation, April 2020
9. A Security Assessment of HTTP/2 Usage in 5G Service Based Architecture; Ericsson research, Sept 2022

# Objective, Scope, and Methodology

## Objective

The FCC tasked CSRIC VIII to examine and address security vulnerabilities associated with the newly adopted 5G signaling protocol, HTTP/2, which, like the SS7 and Diameter signaling protocols considered in earlier CSRICs, may be vulnerable to attacks. There is existing research where the HTTP/2 (and its predecessor HTTP/1.1) have vulnerabilities that put websites on the open Internet at risk. It is important to note that the vulnerabilities are applicable to networks on an open network accessible from the public Internet. They may or may not be applicable to closed networks such as 5G.

The task, delegated to Working Group 1 (WG1), is to research these vulnerabilities and identify others in a 5G context, assess their potential for harm, and recommend safeguards to harden 5G networks and protect critical business and consumer data from these and other cyber threats. In this report, the group provides recommendations on how to remediate the risks associated with HTTP/2.

## Scope

The scope of this report is to consider specific and named vulnerabilities and risk mitigation concerning HTTP/2 and applicability to 5G networks including the following vulnerabilities provided by the FCC:

* + Slow Read attacks, which call on a malicious client to read responses very slowly;
  + HPACK Bombs, which are malicious archive files designed to crash the program or system reading them and often disable antivirus software;
  + Dependency Cycle attacks, which exploit a new flow mechanism designed to optimize networks to instead create an infinite loop which cannot be escaped; and
  + Stream Multiplexing Abuse, which uses security flaws in stream multiplexing functionality to crash servers, resulting in a denial of service to legitimate users.

The group has researched these as well as other vulnerabilities and attack vectors identified by industry through industry SMEs and member expertise.

Consistent with previous CSRIC reports for Signaling System 7 and Diameter protocols[[2]](#footnote-3), this report focuses on signaling protocol vulnerabilities and related usage of HTTP/2 and does not address specific implementations. This report also assumes use of previous recommendations from CSRIC 5G Reports.[[3]](#footnote-4)

## Methodology

The group convened virtual meetings (initially biweekly) to:

* + Research/examine HTTP/2 security vulnerabilities and attack vectors,
  + Engage SMEs to provide input to the group members regarding vulnerabilities, and
  + Review initial set of vulnerabilities and mitigation.

The group provided its findings in two reports:

1. Report on Security Vulnerabilities in HTTP/2, published September 2022, and
2. This report titled Best Practices to Mitigate Vulnerabilities in HTTP/2, published June 2023.

## Presentations from Subject Matter Experts

WG1 received presentations for both reports from four SMEs. These presentations covered research on HTTP vulnerabilities and work from the research community. The following SMEs presented their research:

* James Kettle, Portswigger
* Cathal McDaid, AdaptiveMobile
* Mirja Kuhlewind, Ericsson
* Hyame Alameddine, Ericsson

The working group members expressed their gratitude for the insights and information presented.

# Background and Related 5G Security Activities

## **Use of HTTP/2 Protocols in 3GPP Systems**

Prior to 5G, HTTP/2 was not specified to be used in 3GPP standards based systems. These previous versions of networks used telecommunications-specific Signaling System 7 (SS7) (2G and 3G) and later the Diameter protocol (4G) for signaling. The 3GPP adopted HTTP/2 for signaling due to the architecture required to support the requirements of 5G and future networks.

The two primary usages of HTTP/2 specified within 3GPP standards are for the Service Based Architecture (SBA) and the Service Based Management Architecture (SBMA).

The SBA and SBMA enable the virtualization of Network Functions (NFs) as described in the subsequent sections of this report. Both Virtual Network Functions (VNF) and Containerized Network Functions (CNF) may be used. VNF is Virtual Machine hypervisor-based virtualization. CNF is container-based OS level virtualization.

The 3GPP standards organization has specified HTTP/2 specifically for use in the SBA and SBMA, however, other organizations have specified the use of HTTP/2 for other aspects of 5G. For example, GSMA specifies the use of HTTP/2 for roaming between networks in its 5GS roaming guidelines[[4]](#footnote-5). These recommendations specify the use and treatment of signaling by Internet Packet Exchanges (IPXs). GSMA is also specifying other HTTP/2 uses in the 5G network such as interfaces for [eSIM management](https://www.gsma.com/esim/resources/sgp-21-architecture-specification-v3-0/). Open Radio Access Network (O-RAN) Alliance specifies the use of HTTP/2 for orchestration and management interfaces in the RAN.

The 3GPP SA3 working group has identified several security requirements for a 5G system (5GS) taking into account previous vulnerabilities realized in SS7 and Diameter signaling. These security specifications are not directed specifically at the HTTP/2 protocol, but across the entire network. There are also a set of specifications for each of the network functions in a 5G network that may include HTTP/2 specific requirements.

## 3GPP Service Based Architecture (SBA) Overview

Prior to 5G, interfaces within the 3GPP system were primarily defined as point-to-point interfaces between functions. As the network became more dynamic with virtualization and increased numbers of functions, maintenance of point-to-point interfaces became unsustainable. For 5G, 3GPP adopted the Service Based Architecture (SBA). The SBA is specified in 3GPP TS 23.501[[5]](#footnote-6).



Figure 5.2- Routing Architecture using the Service Based Architecture from 3GPP TS 23.501 (SCP not shown for simplification purposes, please refer to 3GPP 33.501 Standard)

This architecture is composed of a multitude of network functions (NFs) that communicate over a common service based interface (SBI) message bus. Some of the key features of SBA are:

* Direct and Indirect communication and delegated discovery through service communication proxy (SCP).
* Introduction of network functions (NF) sets and NF Service sets – for 5GC the control plane functionality and common data repositories of a 5G network are delivered by way of a set of interconnected network functions, each with authorization to access each other’s services or sets of services.
* Selection and reselection within a NF set – the 5GC employs a centralized discovery selection framework that leverages a network repository function (NRF). The NRF maintains a record of available NF instances and their supported services. It allows other NF instances to subscribe and be notified of registrations from NF instances of a given type. The NRF supports service discovery, by receipt of discovery requests from NF instances and details which NF instances support specific services.
* Convert IMS interfaces to utilize SBA – The 5GC provides the mechanism to convert today’s IP multi-media sub-system (IMS) to use of an SBA that provides flexibility and scale in service delivery as well as support for new capabilities such as network slicing.

The protocol selected for SBI was Representational State Transfer (REST) using HTTP/2. HTTP/2 is the lowest version of the HTTP protocol allowed under SBA specifications.

## 3GPP Service Based Management Architecture Overview

Prior to 5G the management architecture was comprised of two management functions, namely an element manager and a network manager, with a reference point between them, labeled ltf-N, for which management interfaces were defined. Starting with 5G a new management architecture was introduced which moved away from the previous reference point based architecture and adopted a service based architecture, known as the service based management architecture (SBMA).

The SBMA is comprised of a set of management services (MnS) which produce and consume management services such as configuration, performance and fault management with additional services being added with new 3GPP releases. One notable difference between the SBMA and the SBA defined for the 5G Core is that for the most part SBMA services are not tied to a network function whereas with the SBA they are. For example, all 5G core network functions each have their own set of specific services that are strictly associated with a specific NF Type i.e. AMF has its own services, PCF has its own services and so on. The reason the SBMA adopted this approach was to provide as much flexibility as possible and hence encourage innovation such that vendors of management solutions could decide themselves what MnS’s their solutions incorporated without compromising multi-vendor interoperability as all MnS’s are standardized by 3GPP.

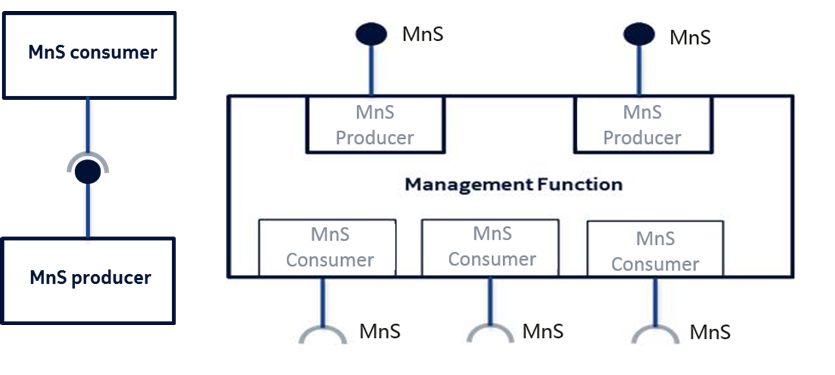


Figure 5.3: MnS Producer, Consumer & Management Function Overview

The SBMA defines a managed object model for each entity that it manages, which is referred to as a network resource model (NRM). For example NRM’s are defined for 5GC NFs such as AMF, for 5G RAN gNB’s and network slice entities such as network slice and network slice subnet instances, which enable management of configuration data as well as performance and fault management data. Services are invoked between MnS consumers and producers via a set of operations and notifications. More details are available about the 3GPP SBMA in the following white paper titled “The 3GPP defined Service Based Management Architecture White Paper (Nokia Bell Labs)”[[6]](#footnote-7).

## Standardization of HTTP and HTTPS in IETF

Hypertext Transfer Protocol (HTTP) is a set of standards allowing internet users to access and retrieve website information. There have been four HTTP iterations since its introduction in 1991. HTTP/2 was released in 2015 as a major revision and replacement for the HTTP/1.1 protocol. It was developed as a way to improve efficiency and online latency and speed. HTTP Secure (HTTPS) is the secure version of the HTTP protocol that uses TLS for encryption and authentication.

HTTP/2 is standardized in RFC 7540 and Hypertext Transfer Protocol Secure (HTTPS) is standardized in RFC 2818. HTTPS is optional to use with HTTP/2. When HTTP/2 is used with the HTTPS uniform resource identifier (URI) scheme it uses Transport Layer Security 1.2 (TLS 1.2) standardized in RFC 5246 or Transport Layer Security 1.3 (TLS 1.3) standardized in RFC 8446. If TLS 1.2 is used for HTTPS, HTTP/2 requires a very strictly profiled version of TLS 1.2. TLS 1.2 has numerous insecure options, including the mandatory to implement cipher suite, which HTTP/2 forbids. [IETF RFC 8740](https://datatracker.ietf.org/doc/html/rfc8740) is a minor update to HTTP/2 that forbids TLS 1.3 post-handshake authentication. IETF RFC 9113 (June 2022) is latest version and obsoletes RFC 8740.

HTTP/3 is the third major version of the Hypertext Transfer Protocol used to exchange information on the Internet. The TCP transport introduces latency issues within signaling and so Google has defined a new protocol called Quick UDP Internet Connections (QUIC) that emulates some of the session related features of the TCP protocol using the UDP protocol instead. UDP runs much faster than TCP sessions but is “best effort”. QUIC provides support for session related communications over the connection-less UDP protocol.

This has not yet been endorsed by 3GPP for use in 5G networks. There is still work underway in the IETF where the HTTP/3 and QUIC protocols are being defined, and 3GPP is waiting for completion of this work.

HTTP/2 allows an option to implement clear text mode which enables trusted middle boxes to eavesdrop, modify, and inject HTTP requests and responses. It is not intended to be used for signaling in critical infrastructure like 5G. Optional security is nowadays not seen as acceptable and HTTP/3 mandates encryption and integrity protection based on TLS 1.3. Mandatory authentication, encryption, and integrity protection aligns with zero-trust principles.

## HTTP/2 and HTTPS in 5G standards

3GPP standards development relies on IETF internet standards[[7]](#footnote-8) for HTTP/2. 3GPP has specified HTTP/2 in all the service based interfaces inside a mobile network as well as between security edge protection proxies (SEPPs) in different mobile networks (N32-c and N32-f interface), according to 3GPP TS 29.500 and TS 29.573. An additional example is between the SEPP and IPXs (with PRINS - Protocol for N32 Interconnect Security S8HR). 3GPP has not yet adopted HTTP/3 for use in 3GPP networks, but this may change over time.

Security requirements for service-based interfaces are specified in the 3GPP SA3 specification TS 33.501. All service based interfaces shall support the 3GPP TLS profile which mandates mutual TLS in clause 6.2 of TS 33.210. For 3GPP interfaces using TLS, TLS 1.3 is mandatory to support for network nodes since 3GPP Rel-15 and for devices since 3GPP Rel-16. Assuming all implementations follow the 3GPP standards, TLS 1.2 would never be used in the 5G architecture. Some early implementations of 5G network nodes do however only support TLS 1.2.

3GPP currently profiles IETF RFCs and is continuously updating 3GPP security specifications to align with IETF and to replace any obsoleted RFCs.

## Non-Core Usage of HTTP (non-3GPP)

The 3GPP has mandated that nothing lower than HTTP/2 should ever be used for signaling in the 5G core network. The use of the HTTP protocol for other applications outside of signaling in the core network is outside the scope of this report.

# Analysis of Protocol Vulnerabilities’ impact on 5G

HTTP/2 is used in many different environments and to support many different applications, ranging from probably the most widespread and well known such as the World Wide Web, The Internet, and web browsing, to specialized and localized services such as micro-services. As described above, 5G's primary use of HTTP/2 is for SBA and SBMA as an example of a specialized and localized service, limited to operations within the 5G core network.

While it is possible to use the vulnerabilities researched by this report against any Internet connected entity from anywhere in the world, the 5GC is not connected to the open and public Internet. The 5GC is a closed network, accessible only from within its boundaries. It could be possible through an insider attack, but this would require the compromise of the network from within a company’s resources, and while possible, highly unlikely. Nonetheless, we will provide recommendations to counter such insider threats.

Therefore, the first assumption on approaching these vulnerabilities is that the 5G core network has deployed robust network perimeter defenses around the SBA and SBMA functions.

The second assumption is that these vulnerabilities would be second or subsequent stages in a multi-stage attack, where an earlier stage attack was a compromise of SBA or SBMA functions.

The results of applying these assumptions to the HTTP/2 protocol vulnerabilities described below means that some vulnerabilities may not be applicable or have limited impact to the specialized and localized use of HTTP/2 by 5G SBA and SBMA.

## Analysis & Observations

The earliest HTTP versions allowed by 3GPP specifications for the 5G SBMA and SBA architectures differ in that 5G SBMA may support HTTP/1.x and later whereas 5G SBA may only support HTTP/2.x and later.

### Client Initiated Attacks on Servers

These types of attacks enumerated in this section are initiated by HTTP/2 clients against HTTP/2 servers. In the 3GPP SBA terminology, this would be the equivalent of a SBA consumer (client) initiating an attack against a SBA producer (server) which could include via or against the SCP (when using Model C/D deployments) or against the SEPP. In 5G networks, each NF provides a service to another NF, and can therefore be either a producer (server) or consumer (client) of a service.

#### Slow Read Attack

This vulnerability was specified as an example HTTP/2 vulnerability by the Commission’s initial CSRIC VIII Working Group 1 charter.

In a slow read attack, the malicious actor sends valid HTTP requests to a server, but reads responses very slowly, such as at the rate of one byte at a time. By keeping the connection active with these small reads, the attacker prevents the server from timing out the connection. The result is that the server must dedicate resources to each such malicious connection. Eventually the server resources may be overwhelmed or the number of slow read service requests being serviced simply blocks legitimate requests from getting through. This read behavior is not explicitly banned by RFC 7540 (HTTP/2).[[8]](#footnote-9)

#### Slow Post Attack

This vulnerability is related to Slow Read Attack.[[9]](#footnote-10) Difference is that malicious client sends a legitimate HTTP POST request with the header Content-Length specified. Then the attacker starts to send the content in a heavily throttled and slow manner. As a result the server involved in properly established connection keeps the connection open to receive the legitimate request. If the attacker sends large number of such requests they can exhaust the available connection pool and blocks the service for other legitimate users.

Slow post attacks do not require a lot of resources for the attacker, and hence they are easy to launch and hard to mitigate. This read behavior is not explicitly banned by RFC 7540 (HTTP/2).

#### HPACK Bombs

This vulnerability was specified as an example HTTP/2 vulnerability by the Commission’s initial CSRIC VIII Working Group 1 charter.

Dynamic header compression is supported in HTTP/2. RFC 7540 permits the server (sender) to define the maximum size of the header compression table. However, the RFC does not restrict the size of individual headers. In the HPACK bomb attack, the malicious actor inserts a header field that is exactly the size of the HPACK dynamic header table into the dynamic header table, followed by repeated requests to expand that field in the dynamic table. These steps can quickly cause a small amount of request data to result in gigabyte-level storage requirements on the target machine. The result is a denial of service as the server’s available resources are exhausted.[[10]](#footnote-11)

#### Dependency Cycle Attacks

This vulnerability was specified as an example HTTP/2 vulnerability by the Commission’s initial CSRIC VIII Working Group 1 charter.

RFC 7540 allows a stream to be given an explicit dependency on another stream:

*“Each stream can be given an explicit dependency on another stream.*

*Including a dependency expresses a preference to allocate resources*

*to the identified stream rather than to the dependent stream.”*

This capability allows the server to prioritize stream handling. But the dependency graph must be a strict tree, as processing a loop or cycle in the graph can cause unpredictable behavior, such as infinite loops or resource overrun. The result is a denial of service as the server’s available resources are exhausted.[[11]](#footnote-12)

#### Stream Multiplexing Abuse

This vulnerability was specified as an example HTTP/2 vulnerability by the Commission’s initial CSRIC VIII Working Group 1 charter. On review by the working group, it is an implementation vulnerability; see Section 6.1.7 below for more information on implementation vulnerabilities. It is listed here for completeness.

An HTTP/2 stream represents a single request/response cycle. Once this cycle is closed, RFC 7540 requires that the stream identifier is not used again over the same connection. If an implementation fails to follow this RFC requirement, it presents an implementation vulnerability. The result is a denial of service attack.

#### URL Prefix Injection

The value of the scheme header is meant to be 'http' or 'https', but it supports arbitrary bytes. Some implementations use it to construct a URL, without performing any validation. This enables an attacker to override the path and, in some cases, poison the cache or create a Server Side Request Forgery (SSRF) vulnerability. Note that while the door is left open by the RFC, an implementation is susceptible if it lacks such validation; since the specific implementations are not know, this is considered a 'Protocol' level scope.

*“The value of the :scheme pseudo-header…is meant to be 'http' or 'https', but it supports arbitrary bytes. Some systems…used it to construct a URL, without performing any validation. This lets you override the path and, in some cases, poison the cache…”[[12]](#footnote-13)*

While this may at root be an implementation vulnerability (see below), it is included here for more thorough review and classification in the next stage of this effort.

#### Illustration of Client Initiated Attacks on Servers

This sequence illustrates an example of how these SBA customer (client) DOS attacks could be directed against a SBA producer. As mentioned previously since the 5G SBA is a closed network and requires earlier steps to compromise the SBA consumer in this example. These earlier stages of the example attack are not detailed.

Step 1: Attacker compromises or takes control over a SMF instance (consumer) and is now “inside” the SBA.

Step 2: The compromised SMF mounts a SBA DOS attack against the UDM (producer) using the slow read vulnerability described above.

Step 3: The 5G network operations degrade under this UDM attack by the compromised SMF instance.

### Heist Attack

While the work on this vulnerability implicates HTTP/2 (RFC 7540), at root there is a weakness in other protocols and implementation behaviors. As the researchers report,

*“…because SSL/TLS does not hide the length of the clear-text message (a weakness that has been well-known to the security community since 1996) adversaries can directly infer the length of the response before encryption.”[[13]](#footnote-14)*

With this information, and by utilizing details of other protocols and web-browser behavior including handling of 3rd-party cookies, the researchers show the ability to extract encrypted information. The following is the recommended mitigation for the Heist Attack.

1. The 5G Core needs to be continuously scanned for:
   1. Port scans of the Operating System.  A credential scan of OS may be performed on some NFs depending upon business requirements, and
   2. Application layer scan of Network Functions [both Virtual Network Functions and Containerized Network Functions].
2. Once an anomaly is detected, the following actions are taken:
   1. A ticket is generated for any vulnerabilities found from the scan,
   2. The Security Operations team contacts the vendor to confirm the vulnerabilities OR to make sure there aren’t any false positives. If no false positives, then start planning to have a timeline to fix the vulnerabilities with the respective vendors, and
   3. Subsequent Lab testing of patch/point release updates that remedies the open scan vulnerabilities.

### Custom HTTP/2 Headers

In addition to the standard HTTP/2 headers, 3GPP has specified several custom headers that are specific to a 5G SBA. Some of these custom headers are defined for flow control and could be used by a compromised NF to slow or shut down critical functions within other NFs[[14]](#footnote-15).

The following non-exhaustive example list of threats involving 3GPP Custom Headers make the assumption that the NF (Network Function) has already been compromised by an adversary. The mitigation to these threats is to ensure that comprehensive monitoring capabilities are in place which can detect and notify the network operator about abnormal NF behavior and hence enable the execution of appropriate mitigation countermeasures e.g. isolate and remove the NF from live service.

The header *3gpp-Sbi-Lci* is used to signal load control information from a producer to a consumer. Misuse of this header could disrupt load balancing within the network, perhaps by directing traffic to the malicious producer even though it is not processing the requests.

The header *3gpp-Sbi-Oci* is used to signal overload control information between producers and consumers. A malicious network function could request that another network function throttle or shut down its requests.

Finally, the header *3gpp-Sbi-Message-Priority* is used to assign priority to a response and could be used by a malicious network function to starve lower priority tasks.

### Implementation Vulnerabilities

Along with the protocol vulnerabilities, there are a number of known vulnerabilities associated with incorrect processing of HTTP/2 traffic. Such issues may be due to failure to follow the protocol specifications correctly, failure to observe good cybersecurity practices such as input data validation, or simply errors in coding. These are typically classified as “bugs” in a product.

These implementation issues do not implicate HTTP/2 systems in general, as do protocol issues. Mitigation for implementation issues is a matter of upgrading to a version of the software provided by the product vendor that has a fix for the issue.

## Best Practices and Recommendations

The scope of this report is the analysis of the identified vulnerabilities and recommended risk mitigations relative to 5G HTTP/2 signaling protocols.

While use of HTTP/1.1 may be common outside of the 5G core network, the known vulnerabilities associated with HTTP/1.1 suggest use of HTTP/2.0 or later versions of the standard is recommended for 5G signaling applications. For use in USA deployments, HTTP/2 is strongly recommended for cybersecurity reasons.

HTTP/2 allows an option to implement clear text mode which enables trusted middle boxes to eavesdrop, modify, and inject HTTP requests and responses. This option is not intended to be used for signaling in critical infrastructure like 5G.

HTTP/2 encryption is on a per JSON Packet basis providing integrity protection, where JSON packets with routing information can be sent with clear text mode, with the payload JSON packets being fully encrypted.

HTTP/2 in 5G Core networks should use encryption and provide integrity protection.

If and when 3GPP adopts HTTP/3, HTTP/3 mandates encryption and integrity protection based on TLS 1.3. Consistent use of authentication, encryption, and integrity protection aligns with zero-trust principles.

Further, this report assumes and recommends that proper security controls and best practices are in place to mitigate threats that may be internal to an organization to detect and mitigate risks and compromise to system credentials and unauthorized access.

In terms of operational segmentation, the group also recommends that operational administrative systems and controls rely on dedicated consoles and not use generic or general purpose devices (e.g. Laptops or PCs) to access administrative and operational systems. Any laptop or PC used to access the Internet or email should never be used for accessing the 5G system.

It is also recommended that monitoring and detection of NF deletion actions require proper escalation, review and approval prior to actual implementation of a deletion request. Given the automated nature of network scaling, this is best accomplished through AI mechanisms that detect multiple NF deletions and can prevent such an activity.

### Client Initiated Attacks on Servers

In the context of public 5G networks, attacks in this Section may not apply because 5G use of HTTP/2 is a closed network and the threat of the attack is unlikely. Both perimeter controls for public 5G networks and other countervailing cybersecurity controls limit the likelihood of such attacks. As is generally the case in 5G, zero-trust principles are assumed, along with proper cybersecurity hygiene where 5G networks do not rely on “open” connections to the internet for HTTP/2. In addition, perimeter security for 5G networks ensures that HTTP/2 protocol connections are not open to the internet and are consistent across server implementations and any network partitioning.

The 5G SBA architecture that relies on HTTP/2 as described in previous sections of this report is a closed network and “air-gapped” with respect to the internet. The SBA is therefore not subject to the threat vectors common in the open internet, e.g. threats to internet browsers. However, insider threats are possible where bad actors can leverage access to functions within the SBA or may implement rogue NFs within the SBA to execute exploits that corrupt network performance. Insider threat mitigation best practices and controls are essential to address such risks (e.g. proper vetting of personnel, least privilege access controls) as well as to detect and mitigate risks and compromise to system credentials and unauthorized access.

As stated previously and in the context of insider threats, the group recommends that operational administrative systems and controls rely on dedicated consoles and not use generic or general purpose devices (e.g. Laptops or PCs) to access administrative and operational systems. Any laptop or PC used to access the Internet or email should never be used for accessing the 5G SBA system.

To reiterate the group recommends the monitoring and detection of NF actions and further require proper escalation, review and approval prior to actual implementation of functional changes to the network.

#### Slow Read Attack: Recommended Mitigation

This vulnerability was specified as an example HTTP/2 vulnerability by the Commission’s initial CSRIC VIII Working Group 1 charter.

Generally speaking, to mitigate this vulnerability the server must recognize the consumption of resources and any mismatch between large requests and small permitted transmits, and take action (e.g., cancel the request) before critical system limits are reached. These parameters are implementation-dependent and will require a heuristic approach by the server implementation developer.

In addition, the original Imperva research noted, “The behavior of servers in Slow Read situations depends on the type and structure of the requests sent…”[[15]](#footnote-16) Consequently, it is not sufficient to simply watch for large requests and small permitted transmits. In that research, two implementations were attacked by repeated requests referencing a resource larger than the remaining window size.[[16]](#footnote-17) Attention must be paid to boundary or edge conditions on requests and implementation behavior.

More specifically, SEPP and SCP server implementations and network integration should consider:[[17]](#footnote-18), [[18]](#footnote-19)

* Server capacity: Upgrading capacity is a stopgap as an aggressive attacker can step up the attack rate to still overwhelm the increased server capacity,
* Reverse-proxy-based protection: This approach is can potentially intercept some of these attacks. A reverse proxy can rate-limit requests on a per-route basis,
* Timeout rules: A connection timeout heuristic can be determined on the statistics of other connections,
* Data rate rules: Enforce a minimum data rate,
* Pattern analysis: An intrusion detection and prevention system using patterns of requests can potentially identify malicious connections, and

Non-specific DDoS mitigations: e.g. segmentation and monitoring.

#### Slow POST Attack: Recommended Mitigation

The attack can be mitigated by:

• Establishing a minimum incoming data rate,

• Ignoring/Dropping any connections that have a rate slower than minimum,

• Setting an absolute connection timeout, and

• Rejecting or drop connections to HTTP methods that are not supported by the server, in order to drop POST messages which are not expected by the service. Note: SCPs / SEPPs cannot say if the target HTTP servers support the specific HTTP methods (and these won’t be able to cache this info for each NF producer / NF consumer for callbacks/notifications).

#### HPACK Bombs: Recommended Mitigation

This vulnerability was specified as an example HTTP/2 vulnerability by the Commission’s initial CSRIC VIII Working Group 1 charter.

The HPACK Bomb attack takes advantage of a server implementation that does not limit unpacked memory in response to requests using HPACK header compression. The mitigation is to set limits, either fixed or dynamic according to some heuristic.[[19]](#footnote-20)

As noted in documentation for the Python Hyper Project “hpack” module, which is a Python interface to an HPACK compression implementation,

*“In version 2.3.0, the HPACK library limits the maximum decompressed size of the header block. It does so by essentially adding support for the HTTP/2 setting SETTINGS\_MAX\_HEADER\_LIST\_SIZE. This value defaults to 64kB, but is user-configurable.”[[20]](#footnote-21)*

#### Dependency Cycle Attacks: Recommended Mitigation

This vulnerability was specified as an example HTTP/2 vulnerability by the Commission’s initial CSRIC VIII Working Group 1 charter.

The Dependency Cycle vulnerability impacts server implantations that support stream prioritization based on dependency weightings. In such cases, there are two elements to mitigation: Prevent dependency cycles and prevent unlimited graph size.

As noted in the original Imperva research,[[21]](#footnote-22)

*“Nghttp2 restricts the dependency graph size to MAX\_CONCURRENT\_STREAMS. When a client tries to create a larger graph using priority frames, the server throws away old streams.”*

However, the server implementation should also restrict dependency graphs to strict tree structure.

It should be noted that an HTTP/2 compliant server implementation is not required to implement the stream prioritization feature. The implementation may ignore client dependency requests or include a server-side option to force stream weightings to default values as per HTTP/2 RFC 9113 Section 5.3.2, *“Default Priorities”*.[[22]](#footnote-23)

#### Stream Multiplexing Abuse: Recommended Mitigation

This vulnerability was specified as an example HTTP/2 vulnerability by the Commission’s initial CSRIC VIII Working Group 1 charter. On review by the working group, it is an implementation vulnerability; see Section 6.2.3 below for more information on implementation vulnerabilities. It is listed here for completeness.

RFC7540 clearly states that for a given connection, “*Stream identifiers cannot be reused.*” In this vulnerability, a flawed implementation fails to observe this requirement consistently. The mitigation is therefore for implementations to follow the RFC in this detail.

#### URL Prefix Injection: Recommended Mitigation

This vulnerability is due to inadequate header field validation. As noted in the PortSwigger research on this topic, the :scheme pseudo-header can include arbitrary data. If that data represents a valid but malicious URL, it can lead to path traversal, code execution and other SSRF consequences.[[23]](#footnote-24)

The mitigation is to perform data validation on all header fields received from the client, but specifically for the arbitrary data in the :scheme pseudo-header. The server should accept only “http”, “https”, or other specific character strings as may be required. The ALPN extension in TLS is also for this purpose, however if the actual :scheme is not as expected then it should be rejected.

### Heist Attack: Recommended Mitigation

The following is the recommended mitigation for the Heist Attack. The 5G Core needs to be continuously scanned and see details in Section 6.1.2.

### Custom HTTP/2 Headers Mitigation

Monitoring of NF functions is recommended to determine if a NF is compromised. The mitigation is to ensure that comprehensive monitoring capabilities are in place which can detect and notify the network operator about abnormal NF behavior and hence enable the execution of appropriate mitigation countermeasures e.g. isolate and remove the NF from live service.

### Implementation Vulnerabilities: Recommended Mitigation

As described above implementation issues do not implicate HTTP/2 systems in general, as do protocol issues. Recommended mitigation for implementation issues is a matter of upgrading to a version of the software provided by the product vendor that has a fix for the issue.

When selecting vendors providing NFs to be used in the 5G system, those NFs should be tested and validated prior to deploying in the network. All NFs should be compliant with the 3GPP Security Assurance Specifications (SCAS) and its evolution for the specific NF.

### General Recommendations

In addition to the previously discussed mitigations, the following are also recommended.

#### Recommendations for Industry

##### Access to 5G Systems

Access to the 5G system should never be through laptops and PCs commonly used for other activities connected to external sources such as the Internet. Only machines dedicated for the use of accessing the 5G system should be used. This is to prevent the introduction of malware from emails or other sources from compromising the machine and making its way into the 5G system (this attack method has already been successful in at least one instance[[24]](#footnote-25)).

##### Latest Network Hygiene

All service providers providing 5G services or maintaining 5G systems should ensure they have practiced the latest network hygiene and implemented the latest security best practices to prevent insider threats.

##### Threat Mitigations

The use of the security threat mitigations outlined in Section 6.2 are recommended.

#### Recommendations for FCC

##### Future CSRIC Considerations

If future evolutions of 3GPP standards make a determination to adopt the usage of HTTP/3 and QUIC, the FCC should consider future CSRIC efforts to study the use of HTTP/3 and QUIC in the context of 5G and future systems.

##### Use of APIs in 5G

A future CSRIC should research the security and vulnerabilities of APIs used within 5G networks, both within the core network or exposed outside the core network.

# Appendix A: Enumerated Protocol Vulnerabilities

The information contained in the following table are examples of protocol vulnerabilities analysis and mitigations that are discussed in aggregate in Section 6.

| **Vuln Name (& a.k.a.)** | **CVE or other ID** | **Overall Type** | **Description** |
| --- | --- | --- | --- |
| **Slow Read (HTTP/2 Flow Control)** | [**CVE-2016-1546**](https://nvd.nist.gov/vuln/detail/CVE-2016-1546) | **DoS** | **Client requests a large amount of data but permits only a small amount (e.g. 1 byte) to be sent at a time. See also CVE-2019-9511, "Data Dribble".** |
| **Slow Read (HTTP/2 Flow Control)** | [**CVE-2020-9481**](https://nvd.nist.gov/vuln/detail/CVE-2020-9481) | **DoS** | **Apache ATS 6.0.0 to 6.2.3, 7.0.0 to 7.1.9, and 8.0.0 to 8.0.6 is vulnerable to a HTTP/2 slow read attack.** |
| **HPACK Bomb** | [**CVE-2016-1544 (also CVE-2016-2525)**](https://nvd.nist.gov/vuln/detail/CVE-2016-1544) | **DoS** | **Per the RFC, each peer can restrict the size of the dynamic header compression table, but does not provide any further restriction on the size of individual headers. Hence, the size of an individual header is only restricted by the scale of the dynamic table. The attack signals a very large dynamic table, then repeatedly opens new streams on the same connection.** |
| **HPACK Bomb** | [**CVE-2016-2525**](https://nvd.nist.gov/vuln/detail/CVE-2016-2525) | **DoS** | **epan/dissectors/packet-http2.c in the HTTP/2 dissector in Wireshark 2.0.x before 2.0.2 does not limit the amount of header data, which allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted packet.** |
| **HPACK Bomb** | [**CVE-2016-6581**](https://nvd.nist.gov/vuln/detail/CVE-2016-6581) | **DoS** | **A HTTP/2 implementation built using any version of the Python HPACK library between v1.0.0 and v2.2.0 could be targeted for a denial of service attack, specifically a so-called "HPACK Bomb" attack. This attack occurs when an attacker inserts a header field that is exactly the size of the HPACK dynamic header table into the dynamic header table. The attacker can then send a header block that is simply repeated requests to expand that field in the dynamic table. This can lead to a gigantic compression ratio of 4,096 or better, meaning that 16kB of data can decompress to 64MB of data on the target machine.** |
| **HPACK Bomb** | [**CVE-2018-5530**](https://nvd.nist.gov/vuln/detail/CVE-2018-5530) | **DoS** | **F5 BIG-IP 13.0.0-13.1.0.5, 12.1.0-12.1.3.5, or 11.6.0-11.6.3.1 virtual servers with HTTP/2 profiles enabled are vulnerable to "HPACK Bomb".** |
| **Dependency Cycle Attack (Dependency and Priority)** | [**CVE-2015-8659**](https://nvd.nist.gov/vuln/detail/CVE-2015-8659) | **Unspecified Impact** | **Per the RFC, a stream may be given an explicit dependency on another stream; this aids in prioritization of stream processing. The dependency graph must be a tree as a cycle in this graph may cause infinite loops or memory overruns (Dependency Cycle Attack). The size of the graph is not limited by the RFC so each server can set its size limitation. The idle stream handling in nghttp2 before 1.6.0 allows attackers to have unspecified impact via unknown vectors, aka a heap-use-after-free bug.** |
| **Data Dribble** | [**CVE-2019-9511**](https://nvd.nist.gov/vuln/detail/CVE-2019-9511) | **DoS** | **The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both, potentially leading to a denial of service.** |
| **URL Prefix Injection** | **N/A** | **Unspecified Impact** | **The value of the scheme header is meant to be 'http' or 'https', but it supports arbitrary bytes. Some system use it to construct a URL, without performing any validation. This lets you override the path and, in some cases, poison the cache or creating a Server Side Request Forgery (SSRF) vulnerability. Note that while the door is left open by the RFC, an implementation is susceptible if it lacks of validation; since the specific implementations are not know, this is considered a 'Protocol' level scope.** |
| **HEIST Attack** | [**CVE-2016-7153**](https://nvd.nist.gov/vuln/detail/CVE-2016-7153) | **Data Exfiltration** | **The HTTP/2 protocol does not consider the role of the TCP congestion window in providing information about content length, which makes it easier for remote attackers to obtain cleartext data by leveraging a web-browser configuration in which third-party cookies are sent, aka a "HEIST" attack.** |

# Appendix B: Glossary of Acronyms

3GPP 3rd Generation Partnership Project

4G Fourth Generation

5G Fifth generation

5GC 5G core

5GS 5G System

AF Application function

AMF Access and mobility function

AN Access Network

API Application Programming Interface

AS Access Stratum

ATIS Alliance for Telecommunications Industry Solutions

AUSF Authentication server function

BGP Border gateway protocol

BITAG Broadband Internet Technical Advisory Group

BSS Base station subsystem

CIoT Cellular Internet of Things

CMMC Cybersecurity Maturity Model Cybersecurity

CP Control Plane

CSA Cloud Security Alliance

CSCC Communications Sector Coordinating Council

CSRIC Communications Security, Reliability and Interoperability Council

CTIA CTIA – The Wireless Association

CU Central unit

DDoS Distributed denial of service

DHS Department of Homeland Security

DU Distributed units

eSIM electronic Subscription Identity Module

ETSI European Telecommunications Standards Institute

FCC Federal Communications Commission

gNB generation Node B

GSMA Global System for Mobile Communications Association

GTP GPRA Tunneling Protocol

HPACK Dynamic Header Packing

HTTP Hypertext Transfer Protocol

ICT Information and Communications Technology

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IMSI International Mobile Subscriber Identity

IoT Internet of Things

IP Internet protocol

IPX Internet Packet Exchange

IPSec Internet Protocol Security

ISP Internet service providers

IT Information technology

ITU International Telecommunication Union

LTE Long-term evolution

MnS Management Services

NEF Network exposure function

NF Network functions

NFV Network function virtualization

NGC Next generation core

NGMN Next Generation Mobile Network

NG-RAN Next generation radio access network

NH Next Hop

NIST National Institute of Standards and Technology

NR New Radio

NPRM Notice of Proposed Rulemaking

NRF Network resource function

NRM Network Resource Model

NSA Non-standalone

NSSAI Network Slice Selection Assistance Information

NSSF Network slice selection function

PBCH Physical broadcast channel

PCF Policy control function

PCFICH Physical control format indicator channel

PCI Physical cell identity

PCRF Policy and charging rules function

PGW Packet gateway

PLMN Public Land Mobile Network

QUIC Quick UDP Internet Connections

RAN Radio Access Network

SA Standalone

SA3 Security working group

SAE System Architecture Evolution

SBA Service-based architecture

SBMA Services Based Management Architecture

SEPP Secure Edge Protection Proxy

SS7 Signaling system 7

SSB Synchronization signal block

SSS Secondary synchronization signal

SST Slice/Service type

SUPI Subscription Permanent Identifier

TAU Tracking Area Update

TLS Transport Layer Security

TS Technical Specification

UDM Unified data management

UE User equipment

UMTS Universal Mobile Telecommunications System

UPF User plane function

URL Uniform Resource Locator

URLLC Ultra-reliable low-latency communication

URI Uniform Resource Identifier

VLR Visitor location register

WG Working Group

1. CSRIC VIII Report on Vulnerabilities in HTTP-2, Sept 2022 https://www.fcc.gov/file/23840/download [↑](#footnote-ref-2)
2. CSRIC VII Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture, December 2020. <https://www.fcc.gov/file/20181/download> [↑](#footnote-ref-3)
3. CSRIC VII Report on Recommendations for Identifying Optional Security Features that can Diminish the Effectiveness of 5G Security, March 2021. <https://www.fcc.gov/file/20606/download> [↑](#footnote-ref-4)
4. GSM Association Official Document: NG.113 - 5GS Roaming Guidelines [NG.113-v4.0.pdf (gsma.com)](https://www.gsma.com/newsroom/wp-content/uploads/NG.113-v4.0.pdf) [↑](#footnote-ref-5)
5. ETSI 3rd Generation Partnership Project Technical Specification: [TS 123 501 - V16.6.0 - 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.6.0 Release 16) (etsi.org)](https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf) [↑](#footnote-ref-6)
6. *See* Nokia Bell Labs, The 3GPP-defined Service Based Management Architecture, 2020. <https://onestore.nokia.com/asset/207723> [↑](#footnote-ref-7)
7. See: 3GPP, A Global Initiative: [Specifications (3gpp.org)](https://www.3gpp.org/specifications). Last Viewed June 08, 2023. [↑](#footnote-ref-8)
8. IMPERVA, Hacker Intelligence Initiative Report, HTTP/2: In-depth Analysis of the Top Four Flaws of the Next Generation Web Protocol, https://www.imperva.com/docs/Imperva\_HII\_HTTP2.pdf [↑](#footnote-ref-9)
9. NetScout, *Slow post attacks,* <https://www.netscout.com/what-is-ddos/slow-post-attacks>, Educative, *What is slow HTTP post DOS attack?*[https://www.educative.io/answers/what-is-slow-http-post-dos-attack](https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.educative.io%2fanswers%2fwhat-is-slow-http-post-dos-attack&c=E,1,6EmnCafk_lfC3wcNLz8He135eOko42hSZP0J9ukqm3NpgnHUhWuatQUjDcG06tk4sFYu_H9IuD2Yh8sTawIdBMxeP-l31LTZg-1Y8LD5mnX9vJwAHA,,&typo=1) [↑](#footnote-ref-10)
10. *Ibid.* [↑](#footnote-ref-11)
11. *Ibid.* [↑](#footnote-ref-12)
12. James Kettle, *HTTP/2: The Sequel is Always Worse*, PortSwigger (August 2022). <https://portswigger.net/research/http2#primitives> [↑](#footnote-ref-13)
13. Mathy Vanhoef and Tom Van Goethem, *HEIST: HTTP Encrypted Information can be Stolen through TCP-windows*, Heist (2016). <https://tom.vg/papers/heist_blackhat2016.pdf> [↑](#footnote-ref-14)
14. IEEE, *A Security Assessment of HTTP/2 Usage in 5G Service-Based Architecture* <https://ieeexplore.ieee.org/document/9952199> [↑](#footnote-ref-15)
15. IMPERVA, Hacker Intelligence Initiative Report, HTTP/2: In-depth Analysis of the Top Four Flaws of the Next Generation Web Protocol, https://www.imperva.com/docs/Imperva\_HII\_HTTP2.pdf [↑](#footnote-ref-16)
16. Ibid. [↑](#footnote-ref-17)
17. NetScout, *Slow read DDoS attack,* https://www.netscout.com/what-is-ddos/slow-read-attacks [↑](#footnote-ref-18)
18. https://www.howtogeek.com/devops/what-is-a-reverse-proxy-and-how-does-it-work/ [↑](#footnote-ref-19)
19. IMPERVA, Hacker Intelligence Initiative Report, HTTP/2: In-depth Analysis of the Top Four Flaws of the Next Generation Web Protocol, https://www.imperva.com/docs/Imperva\_HII\_HTTP2.pdf [↑](#footnote-ref-20)
20. https://python-hyper.org/projects/hpack/en/stable/security/CVE-2016-6581.html [↑](#footnote-ref-21)
21. IMPERVA, Hacker Intelligence Initiative Report, HTTP/2: In-depth Analysis of the Top Four Flaws of the Next Generation Web Protocol, https://www.imperva.com/docs/Imperva\_HII\_HTTP2.pdf [↑](#footnote-ref-22)
22. See Reference 7 [↑](#footnote-ref-23)
23. James Kettle, *HTTP/2: The Sequel is Always Worse*, PortSwigger (August 2022). https://portswigger.net/research/http2 [↑](#footnote-ref-24)
24. [Vodafone Portugal hit with cyberattack affecting 4G/5G network, TV, SMS services | ZDNET](https://www.zdnet.com/article/vodafone-portugal-hit-with-cyberattack-affecting-4g5g-network-tv-sms-services-and-more/) [↑](#footnote-ref-25)