Trend Research

TREND MICRO | CTONE

# Outside Looking In

## How a Packet Reflection Vulnerability Could Allow Attackers to Infiltrate Internal 5G Networks

**Salim S. I.**
CTOne

With Contributions From

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

# Contents




Published by
**Trend Micro Research**



Written by
**Salim S. I.**
*CTOne*

Consider a manufacturing plant where hundreds of internet of things (IoT) devices are connected to the backend with a private 5G network. These devices are in a private IP subnet and are not reachable from external networks. The 5G core is in a cloud, and so are the backend servers. These IoT devices have limited or no internet access.

Since these devices operate in an isolated environment, patching and other security measures may not be up to the mark. There may be an open port listening to commands from backend servers, or there may be a remote code execution (RCE) vulnerability in an embedded web server. But given that they operate in an isolated, NATed, and firewalled private environment, how can an attacker reach them?

The GTP-U between base stations and the user plane function (UPF) of the 5G core lacks encryption and authentication mechanisms. Although the GSM Association (GSMA) recommends Internet Protocol Security (IPSec) encryption on GTP tunnels, this is not often enforced owing to its effects on latency and throughput. In this research, we were able to exploit the GTP-U to attack connected devices from external networks, taking advantage of a packet reflection vulnerability in 5G core UPFs. This security gap is borne from the lack of IP cross-checking between the control and data planes in packet cores. Firewalls and access control lists (ACL) can reduce the attack surface, but these require frequent manual reconfiguring.

The vulnerability detailed in this paper has been reported to Zero Day Initiative (ZDI) and assigned the ID of ZDI-CAN-18522. It rates high in severity as it has a score of 8.3 on the Common Vulnerability Scoring System (CVSS).

This research was done through the cooperative efforts of Trend Micro as the research owner; the Telecom Technology Center (TTC),[1] the official advisory group to Taiwan's National Communications Commission and Ministry of Digital Affairs; and Trend Micro's communication technology (CT) subsidiary CTOne.[2] A cybersecurity leader focused on advancing 5G network security for enterprises, CTOne has served as the researcher in this collaboration alongside TTC, the technical consultant and environment provider through which this research was conducted.

# Enterprise 5G Topologies

Private enterprise 5G may be deployed in different topologies. Most topologies have a local breakout (LBO) at the edge or on-premises, which keeps the local traffic inside company network:

1. 5G core is in a public cloud, with LBO at the edge
2. 5G core is located at the operator's premise, with on-premises LBO
3. 5G core is in a private cloud or multi-access edge (MEC) computing, with co-located LBO

Data traffic from 5G user devices (UE) are transferred over GTP tunnels between a base station and the 5G core.

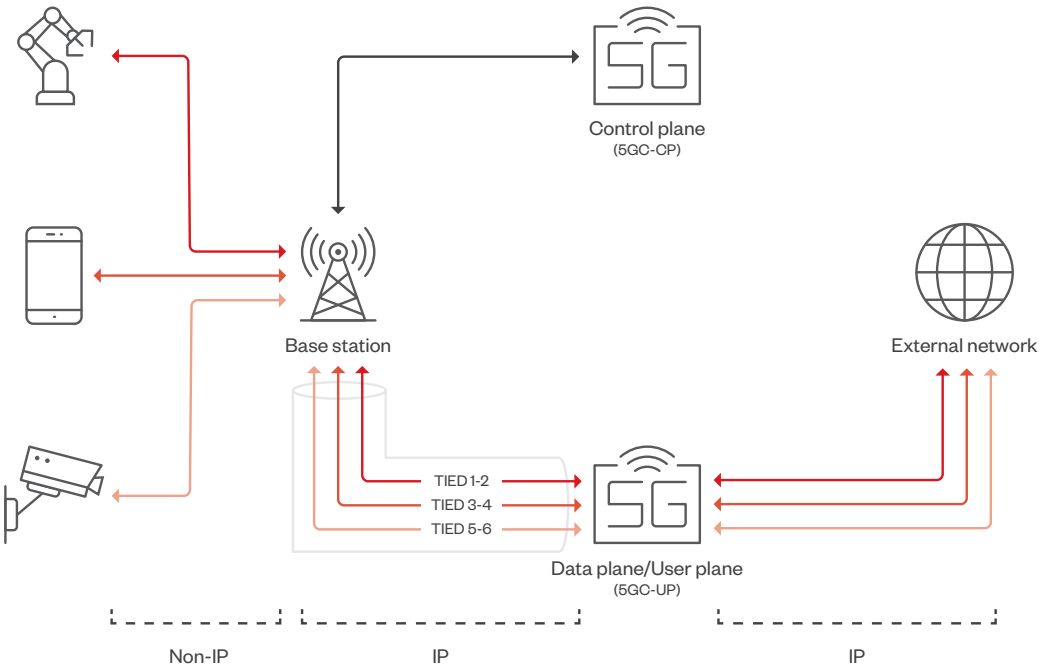


Figure 1. GTP tunnels of various 5G user devices

GTP tunnels are unencrypted user datagram protocol (UDP) tunnels between the 5G core and base stations. Each UE must have at least one GTP tunnel to send or receive traffic. For simplicity, we considered that each UE is allocated two GTP tunnels between base stations and the 5G core: one for uplink packets and one for downlink packets. All sessions of this UE will pass through these tunnels.

5G core-UP identifies a particular tunnel by a 32-bit tunnel endpoint identifier (TEID). For a UE, there is one TEID for uplink and another TEID for downlink. A GTP packet is made by appending a GTP header to the original packet. TEID is part of the GTP header. TEIDs are assigned during Control Channel negotiations.

In summary:

- The tunnel is between base stations and 5G core (GTP nodes)
- UE traffic is encapsulated inside the tunnel

- The GTP tunnel is unencrypted
- The GTP is based on UDP
- The GTP nodes differentiate different tunnels based on TEIDs

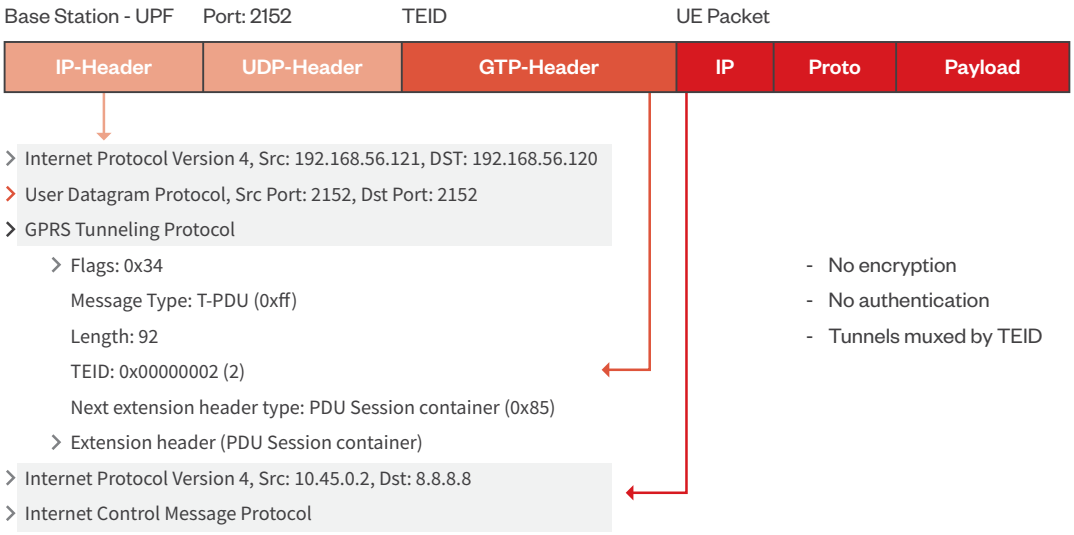


Figure 2. Header information for a GTP tunnel

One characteristic of tunneling is that the inner packet can be delivered unmodified – that is, unaffected by route rules, reverse path filtering, or network address translation (NAT) – across subnets. Combine this with GTP nodes' reliance on TEID for routing GTP tunnels, and we find a potential issue: A GTP packet arriving from anywhere to a 5G core-UP could be processed and its inner packet delivered to a UE if the TEID is valid.

Consider the topology in Figure 3. The control plane IP (CP IP), user plane IP (UP IP), and base station IP (BS IP) are in the 5G core management subnet, whereas the UE is in UE subnet. The UE subnet and management subnet are different and isolated. In private 5G environments, UE subnet is most likely a private subnet.

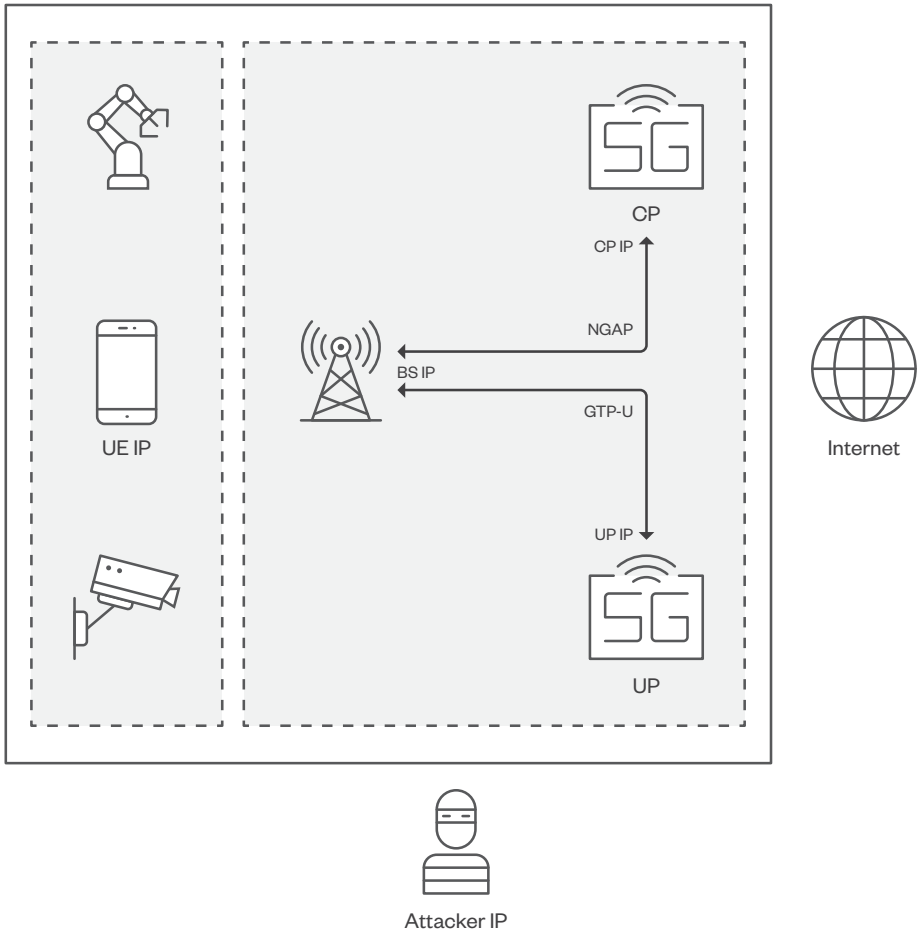


Figure 3. Sample topology of a 5G environment

# Attack Surface

Returning to the original question, how can an attacker reach 5G IoT devices that operate in isolated, NATed, firewalled private environments? One entry point is the 5G core interface itself, which is exposed in the cloud. Since an attack packet with a private address can be tunneled inside a GTP packet, an attacker can craft a GTP packet and send it to the UP IP.

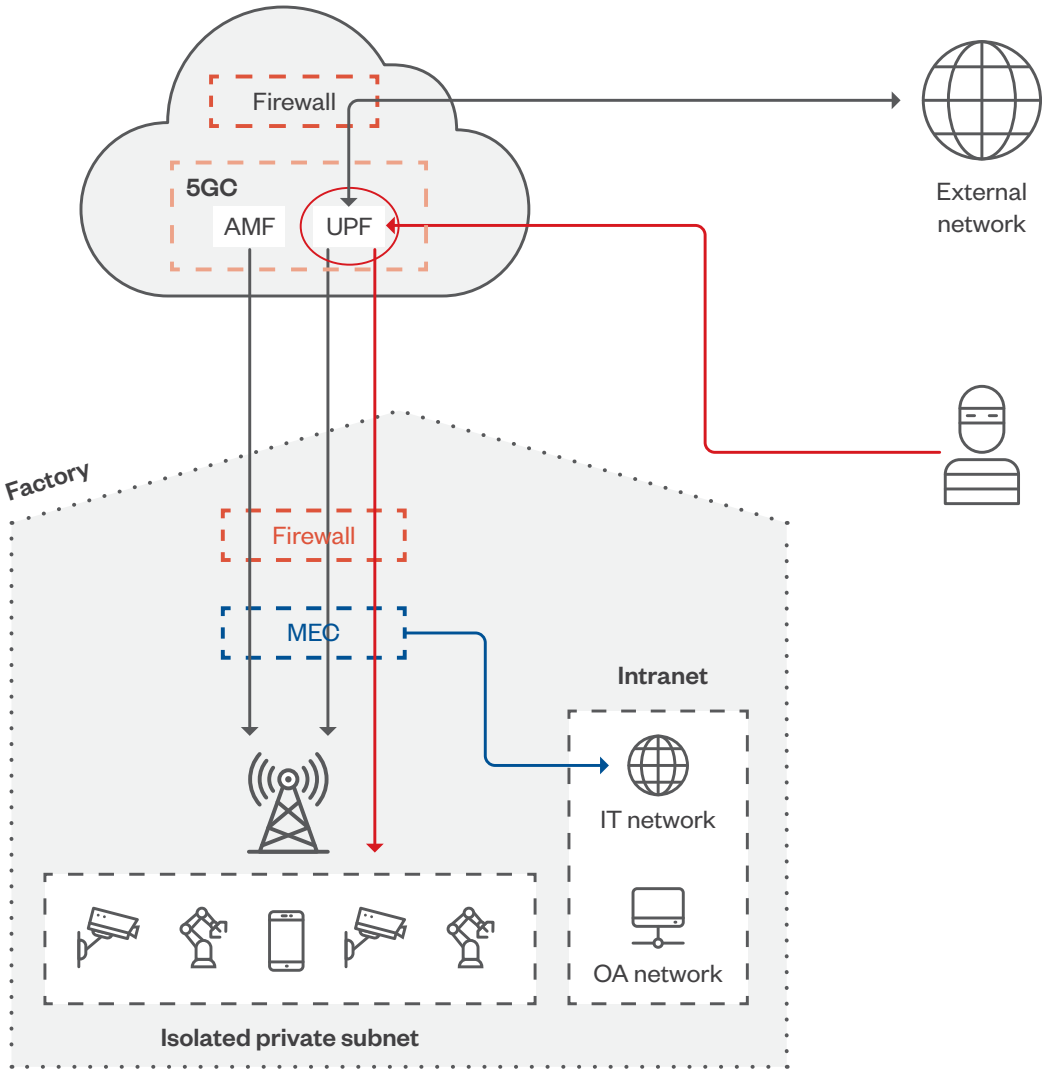


Figure 4. An attacker online can access a private network through a factory's exposed UPF interface

The UPF interface is often exposed to external access due to the nature of certain topologies. Even in telco environments like that of internet service providers (ISPs) and carriers, these interfaces are often exposed to the internet, as detailed further in the Appendix.

# Attack Vectors

## Downlink Packets

In Figure 5, we illustrate one possible attack wherein:

- The attacker creates a packet with the destination as UE IP, the source as an internet IP, encapsulates it in a GTP packet, and sends it to UPF (Arrow 1).
- The UPF looks up the TEID, forwards to base station, which decapsulates the inner packet and forwards it to the corresponding UE (Arrows 2, 3).
- The UE replies to the source IP, i.e. the internet (Arrows 4, 5, 6).

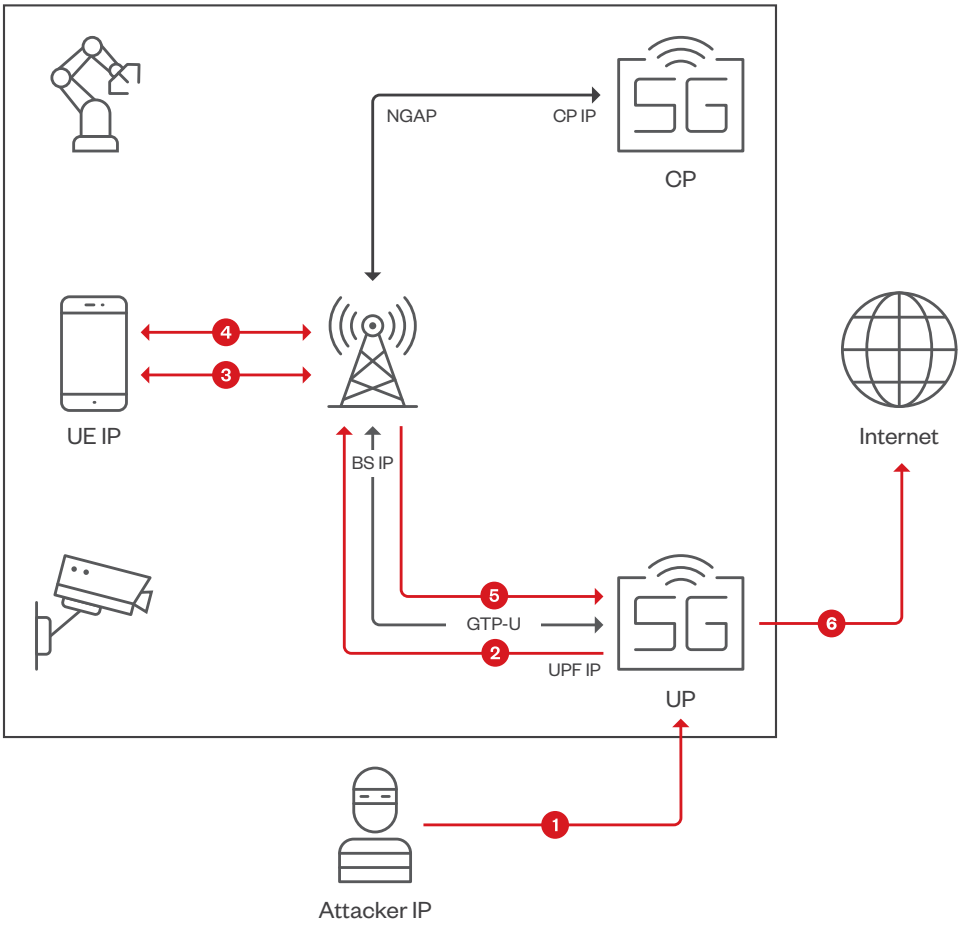


Figure 5. A cyberattack in which the attacker establishes a downlink connection with UE

The Internet IP could very well be the attacker's own IP, thus establishing a two-way connection with the UE (Figure 6). In this case, for the attacker, outgoing packets are GTP and incoming are not.

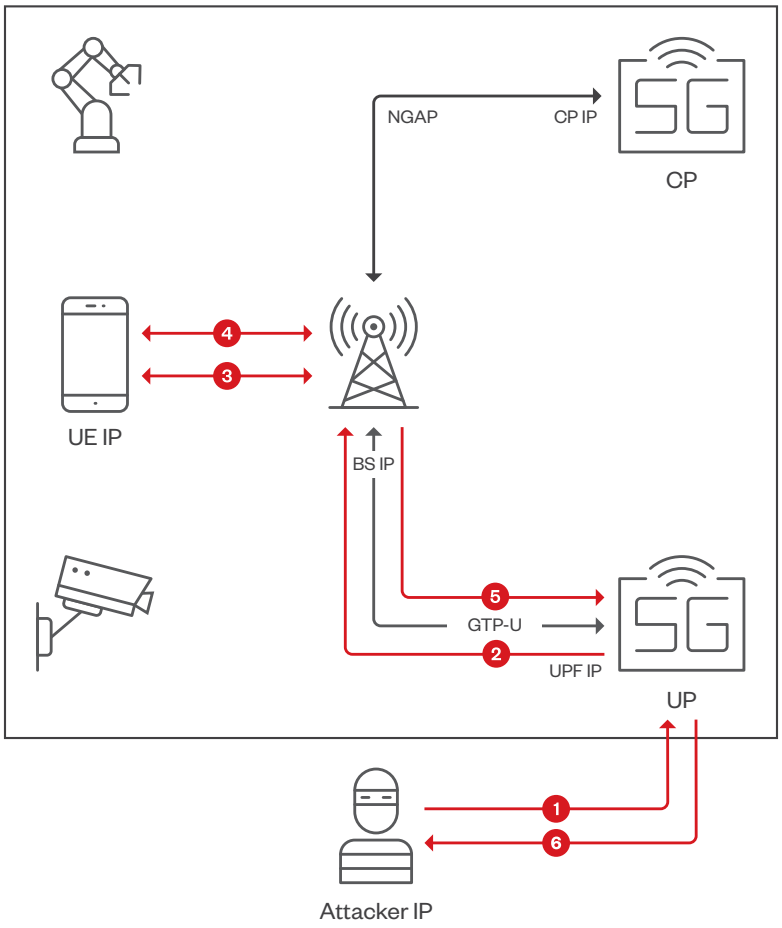


Figure 6. The attacker establishes a two-way connection with user devices, in which outgoing packets are GTP while incoming packets are not

# Uplink Packets

As shown in Figure 7, another way cybercriminals could stage an attack is when:

- The attacker creates a packet with the UE IP as the source, an internet IP as the destination, encapsulates it in a GTP packet, and sends it to UPF (Arrow 1).
- UPF looks up the TEID, decapsulates inner packet, and forwards it to the internet IP (Arrow 2).
- The internet server replies to UE, and it is delivered through 5G network to UE (Arrows 3, 4, 5).

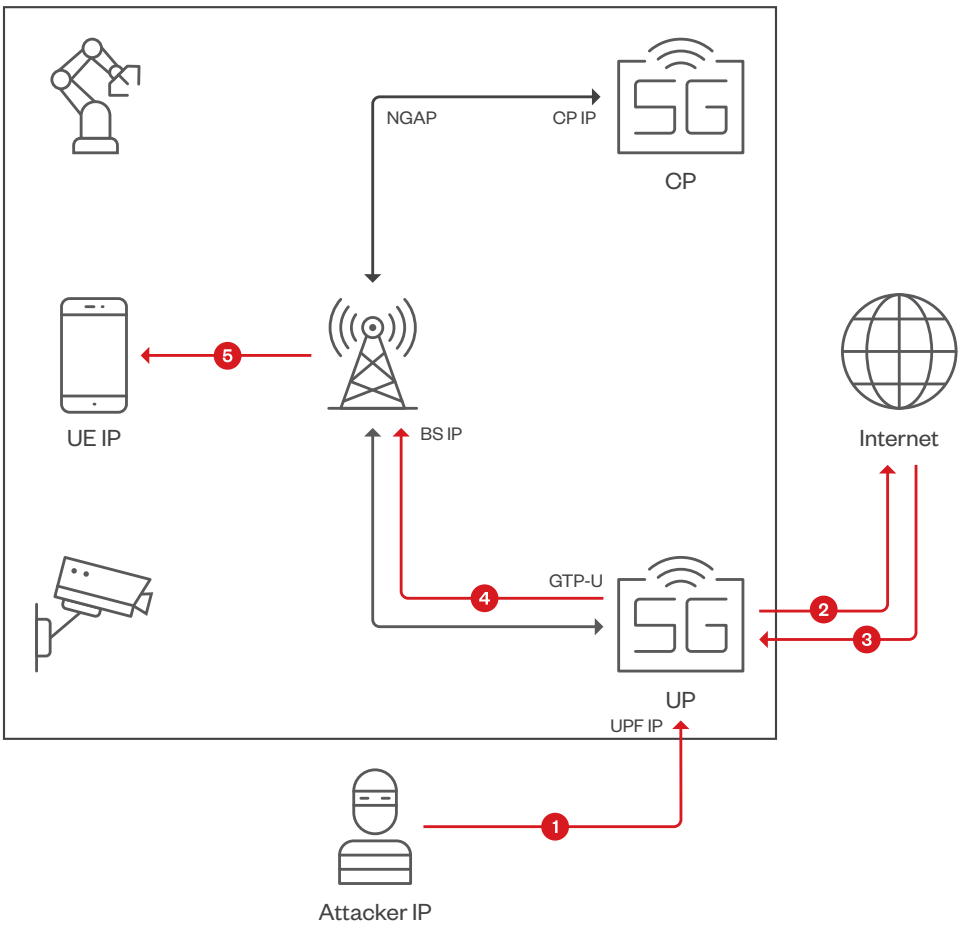


Figure 7. A cyberattack in which attacker establishes an uplink connection on behalf of UE

# TEID Enumeration

For these attacks, a TEID associated with the target IP must be used. TEIDs can be brute-forced: A TEID is 32-bits long and is supposed to be random; however, in practice, some vendors show an affinity toward certain ranges, which can be leveraged in smart guessing. An attacker may send several pings to the target IP, with several different TEIDs in the GTP packet. When a TEID and the IP match, the attacker will receive a ping response.

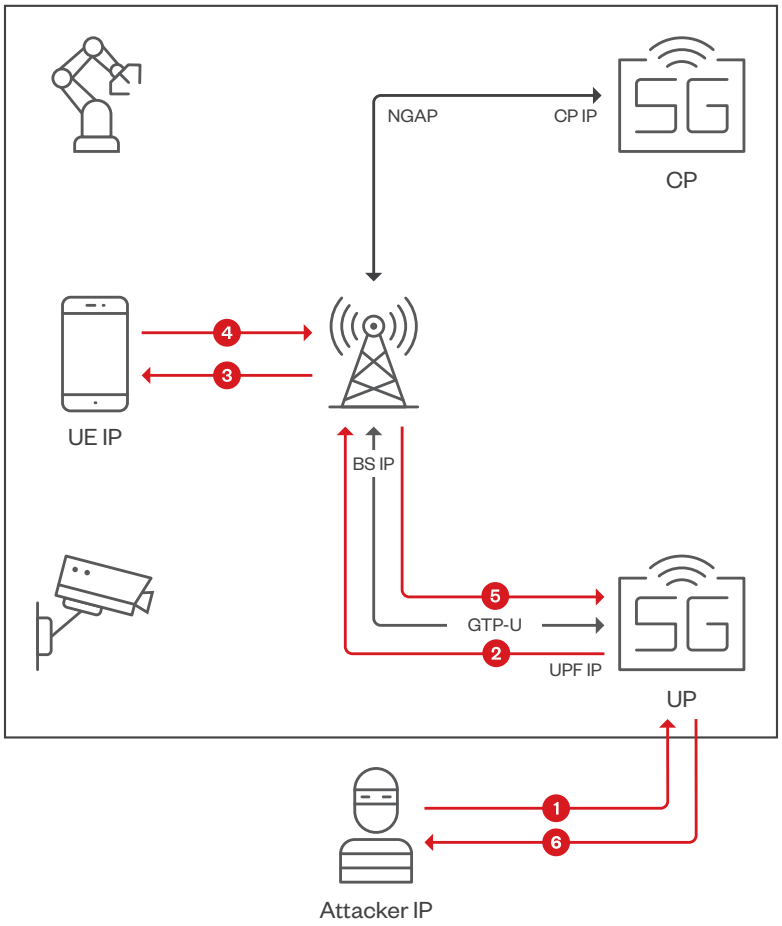


Figure 8. An attacker sending multiple pings to the targeted IP with different TEIDs in the GTP packet

# Root Cause

Ideally, UPF should verify that the packet comes from a trusted peer. However, the 3rd Generation Partnership Project (3GPP) standards do not enforce this verification. Consequently, many vendors do not build in verification mechanisms either. We conducted tests on 5G cores from four vendors: two open-source vendors and two commercial vendors, all of which were found vulnerable.

The GSMA's suggested remediation to protect GTP is to use IPsec between base stations and the 5G core. However, IPsec is rarely used in real deployments because of the costs involving latency, throughput, resources such as CPU and memory, and other monetary costs, especially with regards to scaling.

# Disclosure and Response

One of the devices vulnerable to this attack is an enterprise packet core used in the deployment of private wireless networks. Through ZDI, the vulnerability has been reported to the device's vendor, which recommends that affected users use firewalls and demilitarized zones (DMZs) to protect their 5G cores. From our point of view, this must be considered a vulnerability in the 5G core: If a web server or gateway were reported to have such a vulnerability, preventing attack packets from reaching the web server or gateway would not be an acceptable remedy.

# Conclusion and Recommendations

In summary, an attacker from anywhere on the internet could gain access to a private network using this vulnerability, as illustrated earlier in Figure 4. GTP-U tunneling exposes private subnets to access from external networks, which would enable attackers on external networks to gain a foothold into devices on cellular networks. Multiple commercial 5G cores are open to attack.

This vulnerability should be seen as a door that lets an attacker into an internal network and exploit any vulnerabilities in the network's connected devices. Considering that factory floor equipment is usually in isolated and private networks – and therefore may not always be up to date with security patches – this can affect manufacturers and other kinds of businesses in various ways: it puts their operations at risk of ransomware attacks, exfiltration of sensitive data, hours of disruption from denial-of-service (DoS) attacks, and stealth agents that can lead to poor product quality.

Enterprises can fortify their defenses against this vulnerability through the following security practices:

1. IPsec or other secure tunneling mechanisms can prevent most man-on-the-side (MoTS) attacks, if its various costs of encryption are acceptable for an organization.
2. Since 5G cores from most vendors do not have built-in mechanisms to cross-check IPs, an external security device with this capability will help reduce the attack surface without compromising performance.

Enterprises can also benefit from CTOne, a global cybersecurity leader in communication technology, offers enterprise cybersecurity solutions for next-generation wireless networks. A subsidiary of Trend Micro, CTOne enables digital transformation and strengthens the resilience of communication technology.

Multilayered security solutions such as Trend Vision One™,[3] a cybersecurity platform, can help businesses protect their infrastructure. Trend Vision One provides enterprises with a holistic view of their attack surface and streamlined detection and response that's adaptive to ICS and 5G. It assesses their risk exposure and automatically deploys controls to mitigate those risks, leading to fewer, higher-fidelity alerts that free up security teams to work on strategically important tasks.

As more companies adopt private 5G networks for their low latency, large bandwidth, and high-density capabilities, they will need to protect their factory environments from potential cyberattacks. To this end, Trend Micro's ICS/OT Security[4] offers solutions that are built on exhaustive threat intelligence and expertise from ZDI, TXOne Networks, and Trend Micro Research. Its suite of IT-, OT-, and CT-integrated solutions enable early threat detection and response while cutting down on monitoring complexity, empowering manufacturers to better defend their industrial IT ecosystem.

# Appendix

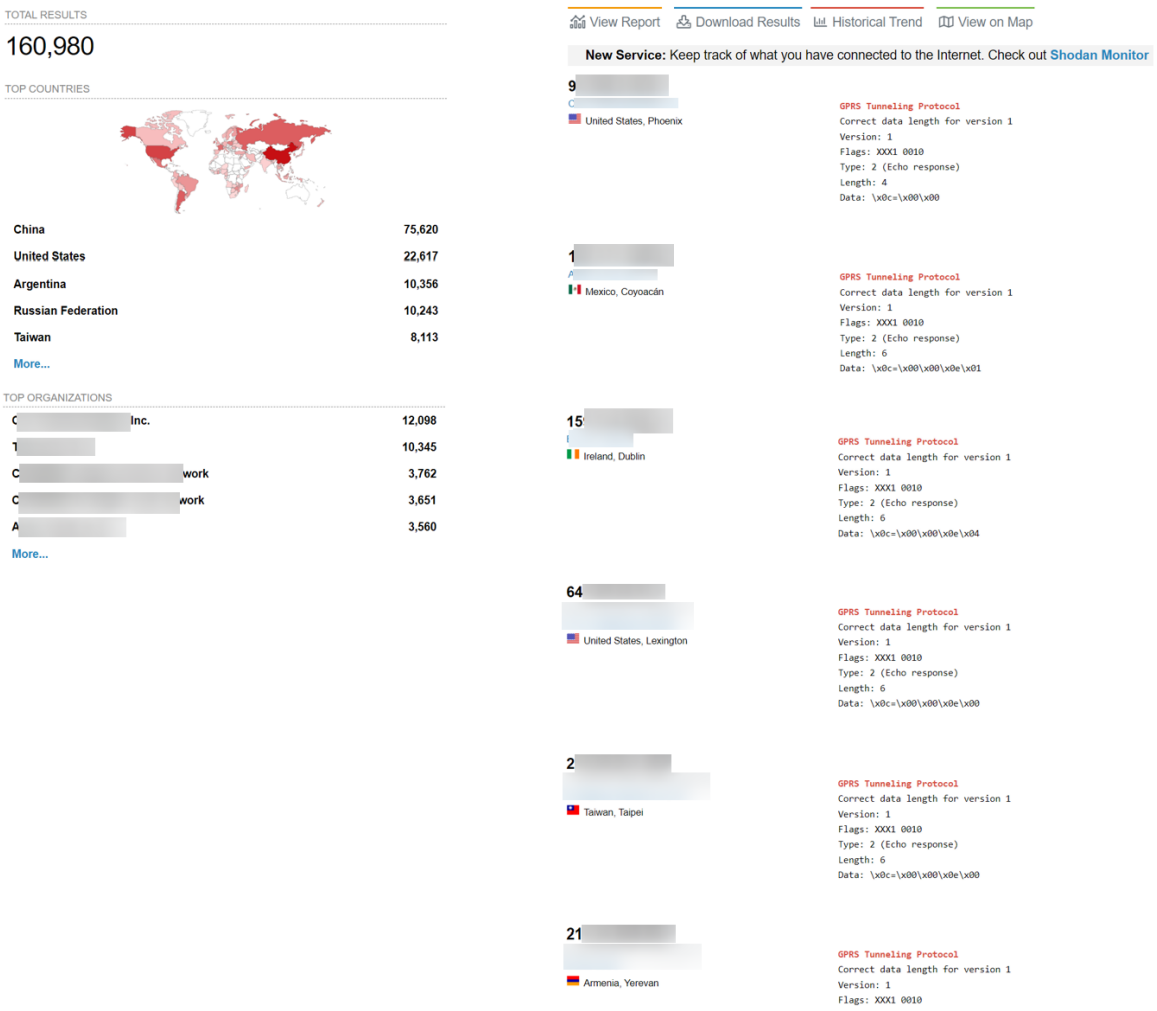


Figure 9. Top countries with exposed UPF interfaces

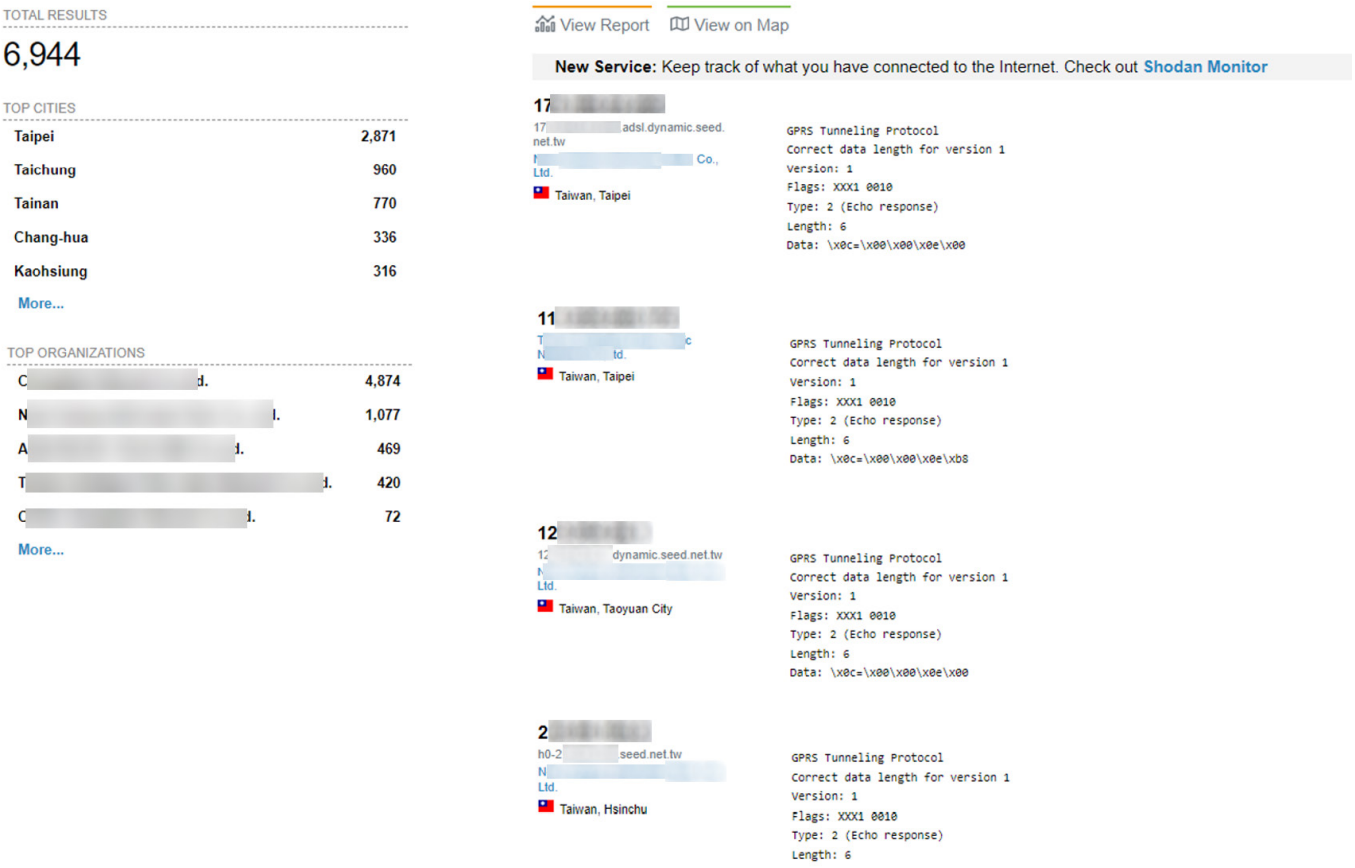


Figure 10. Top cities in Taiwan with exposed UPF interfaces

# Endnotes


1 Telecom Technology Center. (n.d.). *Telecom Technology Center*. "About TTC." Accessed on Apr. 17, 2023, at Link.

2 CTOne. (n.d.). *CTOne*. "About CTOne." Accessed on Apr. 17, 2023, at Link.

3 Trend Micro. (n.d.). *Trend Micro*. "Trend Vision One™." Accessed on July 6, 2023, at Link.

4 Trend Micro. (n.d.). *Trend Micro*. "ICS/OT Security." Accessed on Apr. 17, 2023, at Link.


For more information visit **trendmicro.com**