Record breaking DDoS Potential Discovered: CVE-2022-26143

team-cymru.com/blog/2022/03/08/record-breaking-ddos-potential-discovered-cve-2022-26143/

James Shank View all posts by James Shank March 8, 2022

CVE-2022-26143: TP240PhoneHome Reflection/Amplification DDoS Attack Vector

Executive summary

- A new reflection/amplification distributed denial-of-service (DDoS) vector with a record-breaking potential amplification ratio of 4,294,967,296:1 has been abused by attackers in the wild to launch multiple high-impact DDoS attacks.
- Security researchers, network operators, and security vendors observed these attacks and formed a task force to investigate the new DDoS vector and provide mitigation guidance.
- Approximately 2,600 Mitel MiCollab and MiVoice Business Express collaboration systems acting as PBX-to-internet gateways were incorrectly deployed with an abusable system test facility exposed to the public internet.
- Attackers were actively leveraging these systems to launch reflection/amplification DDoS attacks of more than 53 million packets per second (Mpps). With optimal attack tuning, the potential traffic yield for this DDoS vector is significantly higher.
- Attacks have been observed on broadband access ISPs, financial institutions, logistics companies, gaming companies, and organizations in other vertical markets.
- The attacks can be mitigated using standard DDoS-defense techniques.
- Mitel has released patched software that disables the abusable test facility, and is actively engaged in remediation efforts with their customers.
- Research and mitigation task force contributors include Akamai SIRT, Cloudflare, Lumen Black Lotus Labs, Mitel, NETSCOUT Arbor ASERT, TELUS, Team Cymru, and The Shadowserver Foundation.

Introduction

Beginning in mid-February 2022, security researchers, network operators, and security vendors observed a spike in DDoS attacks sourced from UDP port 10074 targeting broadband access ISPs, financial institutions, logistics companies, and organizations in other vertical markets.

Upon further investigation, it was determined that the devices abused to launch these attacks are MiCollab and MiVoice Business Express collaboration systems produced by which incorporate TP-240 VoIP-processing interface cards and supporting software; their primary function is to provide internet-based site-to-site voice connectivity for PBX systems.

Approximately 2600 of these systems have been incorrectly provisioned so that an unauthenticated system test facility has been inadvertently exposed to the public internet, allowing attackers to leverage these PBX VoIP gateways as DDoS reflectors/amplifiers.

Mitel is aware that these systems are being abused to facilitate high-pps DDoS attacks, and have been actively working with customers to remediate abusable devices with patched software that disables public access to the system test facility.

In this blog, we will further explore the observed activity, explain how the driver has been abused, and share recommended mitigation steps. This research was created cooperatively among a team of researchers from Akamai SIRT, Cloudflare, Lumen Black Lotus Labs, NETSCOUT Arbor ASERT , TELUS, Team Cymru, and The Shadowserver Foundation.

DDoS attacks in the wild

While spikes of network traffic associated with the vulnerable service were observed on January 8 and February 7, 2022, we believe the first actual attacks leveraging the exploit began on February 18.

Observed attacks were primarily predicated on pps, or throughput, and appeared to be UDP reflection/amplification attacks sourced from UDP/10074 that were mainly directed toward destination ports UDP/80 and UDP/443. The single largest observed attack of this type preceding this one was approximately 53 Mpps and 23 Gbps. The average packet size for that attack was approximately 60 bytes, with an attack duration of approximately 5 minutes. The amplified attack packets are not fragmented.

This particular attack vector differs from most UDP reflection/amplification attack methodologies in that the exposed system test facility can be abused to launch a sustained DDoS attack of up to 14 hours in duration by means of *a single spoofed attack initiation packet*, resulting in a record-setting packet amplification ratio of *4,294,967,296:1*. A controlled test of this DDoS attack vector yielded more than 400 Mpps of sustained DDoS attack traffic.

It should be noted that this single-packet attack initiation capability has the effect of precluding network operator traceback of the spoofed attack initiator traffic. This helps mask the attack traffic generation infrastructure, making it less likely that the attack origin can be traced compared with other UDP reflection/amplification DDoS attack vectors.

Abusing the tp240dvr driver

The abused service on affected Mitel systems is called tp240dvr (“TP-240 driver”) and appears to run as a software bridge to facilitate interactions with TDM/VoIP PCI interface cards. The service listens for commands on UDP/10074 and is not meant to be exposed to the internet, as confirmed by the manufacturer of these devices. It is this exposure to the internet that ultimately allows it to be abused.

The tp240dvr service exposes an unusual command that is designed to stress test its clients in order to facilitate debugging and performance testing. This command can be abused to cause the tp240dvr service to send this stress test to attack victims. The traffic consists of a high rate of short informative status update packets that can potentially overwhelm victims and cause the DDoS scenario.

This command can also be abused by attackers to launch very high-throughput attacks. Attackers can use specially crafted commands to cause the tp240dvr service to send larger informative status update packets, significantly increasing the amplification ratio.

By extensively testing isolated virtual TP-240–based systems in a lab setting, researchers were able to cause these devices to generate massive amounts of traffic in response to comparatively small request payloads. We will cover this attack scenario in greater technical depth in the following sections.

Calculating the potential attack impact

As previously mentioned, amplification via this abusable test facility differs substantially from how it is accomplished with most other UDP reflection/amplification DDoS vectors. Typically, reflection/amplification attacks require the attacker to continuously transmit malicious payloads to abusable nodes for as long as they wish to attack the victim. In the case of TP-240 reflection/amplification, this continuous transmission is not necessary to launch high-impact DDoS attacks.

Instead, an attacker leveraging TP-240 reflection/amplification can launch a high-impact DDoS attack using a single packet. Examination of the tp240dvr binary reveals that, due to its design, an attacker can theoretically cause the service to emit 2,147,483,647 responses to a single malicious command. Each response generates two packets on the wire, leading to approximately 4,294,967,294 amplified attack packets being directed toward the attack victim.

For each response to a command, the first packet contains a counter that increments with each sent response. As the counter value increments, the size of this first packet will grow from 36 bytes to 45 bytes. The second packet contains diagnostic output from the function, which can be influenced by the attacker. By optimizing each initiator packet to maximize the size of the second packet, every command will result in amplified packets that are up to 1,184 bytes in length.

In theory, a single abusable node generating the upper limit of 4,294,967,294 packets at a rate of 80 thousand packets per second (Kpps) would result in an attack duration of roughly 14 hours. Over the course of the attack, the “counter” packets alone would generate roughly

95.5 GB of amplified attack traffic destined for the targeted network. The maximally padded “diagnostic output” packets would account for an additional 2.5 TB of attack traffic directed toward the target.

This would yield a sustained flood of just under 393 Mbps of attack traffic from a single reflector/amplifier, all resulting from a single spoofed attack initiator packet of only 1,119 bytes in length. This results in a nearly unimaginable amplification ratio of 2,200,288,816:1 — a multiplier of *220 billion percent*, triggered by a single packet.

Upper boundaries of attack volume and simultaneity

The tp240dvr service processes commands using a single thread. This means they can only process a single command at a time, and thus can only be used to launch one attack at a time. In the example scenario presented above, during the 14 hours that the abused device would be attacking the target, it cannot be leveraged to attack any other target. This is somewhat unique in the context of DDoS reflection/amplification vectors.

Although this characteristic also causes the tp240dvr service to be unavailable to legitimate users, it is much preferable to having these devices be leveraged in parallel by multiple attackers — and leaving legitimate operators of these systems to wonder why their outbound internet data capacity is being consumed at much higher rates.

Additionally, it appears these devices are on relatively low-powered hardware in terms of their traffic-generation capabilities. On an internet where 100 Gbps links, dozens of CPU cores, and multithreading capabilities have become commonplace, we can all be thankful this abusable service is not found on top-of-the-line hardware platforms capable of individually generating Mpps, and running with thousands of parallelized threads.

Lastly, it is also good news that of the tens of thousands of these devices that have been purchased and deployed historically by governments, commercial enterprises, and other organizations worldwide, a relatively small number of them have been configured in a manner that leaves them in this abusable state, and of those, many have been properly secured and taken offline from an attacker’s perspective.

Collateral impact

The collateral impact of TP-240 reflection/amplification attacks is potentially significant for organizations with internet-exposed Mitel MiCollab and MiVoice Business Express collaboration systems that are abused as DDoS reflectors/amplifiers.

This may include partial or full interruption of voice communications through these systems, as well as additional service disruption due to transit capacity consumption, state-table exhaustion of network address translations, stateful firewalls, and so forth.

Wholesale filtering of all UDP/10074-sourced traffic by network operators may potentially overblock legitimate internet traffic, and is therefore contraindicated.

During the testing and research phases, an UTRS participant network got hit with an attack and used UTRS to successfully mitigate the attack. The corresponding network graphs are a dramatic testament to the success of UTRS.

More can be found about this Team Cymru Community Service here.

Recommended actions

TP-240 reflection/amplification DDoS attacks are sourced from UDP/10074 and destined for the UDP port of the attacker’s choice. This amplified attack traffic can be detected, classified, traced back, and safely mitigated using standard DDoS defense tools and techniques.

Flow telemetry and packet capture via open-source and commercial analysis systems can alert network operators and end customers of TP-240 reflection/amplification attacks.

Network access control lists (ACLs), flowspec, destination-based remotely triggered blackhole, source-based remotely triggered blackhole, and intelligent DDoS mitigation systems can be used to mitigate these attacks.

Network operators should perform reconnaissance to identify and facilitate remediation of abusable TP-240 reflectors/amplifiers on their networks and/or the networks of their customers. Operators of Mitel MiCollab and MiVoice Business Express collaboration systems should proactively contact Mitel to receive specific remediation instructions from the vendor.

Organizations with business-critical public-facing internet properties should ensure that all relevant network infrastructure, architectural, and operational best current practices (BCPs) have been implemented, including situationally specific network access policies that only permit internet traffic via required IP protocols and ports. Internet access network traffic to/from internal organizational personnel should be isolated from internet traffic to/from public-facing internet properties, and served via separate upstream internet transit links.

DDoS defenses for all public-facing internet properties and supporting infrastructure should be implemented in a situationally appropriate manner, including periodic testing to ensure that any changes to the organization’s servers/services/applications are incorporated into its DDoS-defense plan.

It is imperative that organizations operating mission-critical public-facing internet properties and/or infrastructure ensure that all servers/services/application/datastores/infrastructure elements are protected against DDoS attack, and are included in periodic, realistic tests of the organization’s DDoS mitigation plan. Critical ancillary supporting services such as authoritative and recursive DNS servers must be included in this plan.

Network operators should implement ingress and egress source address validation in order to prevent attackers from initiating reflection/amplification DDoS attacks.

All potential DDoS attack mitigation measures described in this document ***MUST*** be tested and customized in a situationally appropriate manner prior to deployment on production networks.

Mitigating factors

Operators of internet-exposed TP-240–based Mitel MiCollab and MiVoice Business Express collaboration systems can prevent abuse of their systems to launch DDoS attacks by blocking incoming internet traffic destined for UDP/10074 via ACLs, firewall rules, and other standard network access control policy enforcement mechanisms.

Mitel has provided patched software versions that prevent TP-240–equipped MiCollab and MiVoice Business Express collaboration systems from being abused as DDoS reflectors/amplifiers by preventing exposure of the service to the internet. Mitel customers should contact the vendor for remediation instructions.

Collateral impact to abusable TP-240 reflectors/amplifiers can alert network operators and/or end customers to remove affected systems from “demilitarized zone” networks or internet data centers or to disable relevant UDP port–forwarding rules that allow specific UDP/10074 traffic sourced from the public internet to reach these devices, thereby preventing them from being abused to launch reflection/amplification DDoS attacks.

The amplified attack traffic is not fragmented, so there is no additional attack component consisting of non initial fragments, as is the case with many other UDP reflection/amplification DDoS vectors.

Implementation of ingress and egress source-address validation (SAV; also known as anti-spoofing) can prevent attackers from launching reflection/amplification DDoS attacks.

Conclusion

Unfortunately, many abusable services that should not be exposed to the public internet are nevertheless left open for attackers to exploit. This scenario is yet another example of real-world deployments that do not adhere to vendor guidance. Vendors can prevent this situation by adopting “safe by default” postures on devices before shipping.

Reflection/amplification DDoS attacks would be impossible to launch if all network operators implemented ingress and egress SAV (or anti-spoofing). The ability to spoof the IP address(es) of the intended attack target(s) is required to launch such attacks. Service providers must continue to implement SAV in their own networks, and require that their downstream customers do so as well.

As is routinely the case with newer DDoS attack vectors, it appears that after an initial period of employment by advanced attackers with access to bespoke DDoS attack infrastructure, TP-240 reflection/amplification has been weaponized and added to the arsenals of so-called “booter/stresser” DDoS-for-hire services, placing it within the reach of the general attacker population.

Collaboration across the operational, research, and vendor communities is central to the continued viability of the internet. The quick response to and ongoing remediation of this high-impact DDoS attack vector has only been possible as a result of such collaboration. Organizations with a vested interest in the stability and resiliency of the internet should embrace and support cross-industry cooperative efforts as a core principle.

The combined efforts of the research and mitigation task force demonstrates that successful collaboration across industry peers to quickly remediate threats to availability and resiliency is not only possible, but is also increasingly critical for the continued viability of the global internet.

Sources

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26143/

https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-22-0001

https://www.cisa.gov/uscert/ncas/alerts/TA14-017A

https://www.senki.org/ddos-attack-preparation-workbook/

https://www.manrs.org/resources/

https://www.rfc-editor.org/info/bcp84

https://datatracker.ietf.org/doc/html/rfc7039

Research and mitigation task force contributors

Researchers from the following organizations have contributed to the findings and recommendations described in this document:

In particular, the mitigation task force would like to cite Mitel for their exemplary cooperation, rapid response, and ongoing participation in remediation efforts. Mitel quickly created and disseminated patched software, worked with their customers and partners to update affected systems, and supplied valuable expertise as the task force worked to formulate this document.