How malformed packets caused CenturyLink's 37-hour, nationwide outage

reader comments

60 with 46 posters participating, including story author

Share this story

CenturyLink's nationwide, 37-hour outage in December 2018 disrupted 911 service for millions of Americans and prevented completion of at least 886 calls to 911, a new Federal Communications Commission report said.

Back in December, FCC Chairman Ajit Pai called the outage on CenturyLink's fiber network "completely unacceptable" and vowed to investigate. The FCC released the findings from its investigation today, describing how CenturyLink failed to follow best practices that could have prevented the outage. But Pai still hasn't announced any punishment of CenturyLink.

The outage was so extensive that it affected numerous other network operators that connect with CenturyLink, including Comcast and Verizon, the FCC report said. An FCC summary said:

> *The outage affected communications service providers, businesses customers, and consumers who relied upon CenturyLink's transport services, which route communications traffic from various providers to locations across the country. The outage resulted in extensive disruptions to phone and broadband service, including 911 calling. As many as 22 million customers across 39 states were affected,*

> *including approximately 17 million customers across 29 states who lacked reliable access to 911. At least 886 calls to 911 were not delivered.*

The 37-hour outage began on December 27 and "was caused by an equipment failure that was exacerbated by a network configuration error," the FCC said. CenturyLink estimates that more than 12.1 million phone calls on its network "were blocked or degraded due to the incident," the FCC said.

Additionally, about 1.1 million of CenturyLink's DSL customers lost service for parts of the 37 hours. Another 2.6 million DSL customers "may have experienced degraded service," the FCC said.

Pai today again called the outage "completely unacceptable" and said "it's important for communications providers to take heed of the lessons learned from this incident."

But the FCC didn't announce a punishment or even an order requiring CenturyLink to take specific steps to upgrade its network. Instead, the FCC said it "will engage in stakeholder outreach to promote best practices and contact other major transport providers to discuss their network practices," and "offer its assistance to smaller providers to help ensure that our nation's communications networks remain robust, reliable, and resilient." The FCC said it will also issue a public notice "reminding companies of industry-accepted best practices."

We asked Pai's office today if he's planning any disciplinary action against CenturyLink, and we will update this article if we get a response.

While Pai's FCC deregulated broadband when it repealed net neutrality rules, it still regulates landline phone networks such as CenturyLink's with its Title II authority over common carriers.

When contacted by Ars, Democratic FCC Commissioner Jessica Rosenworcel said the report should have been completed sooner and that it should have included “an action plan to avoid a repeat. It’s a real problem [that] there is no such plan here.”

Root cause

Problems began the morning of December 27 when “a switching module in CenturyLink’s Denver, Colorado, node spontaneously generated four malformed management packets,” the FCC report said.

CenturyLink and Infinera, the vendor that supplied the node, told the FCC that “they do not know how or why the malformed packets were generated.”

Malformed packets “are usually discarded immediately due to characteristics that indicate that the packets are invalid,” but that didn’t happen in this case, the FCC report explained:

> *In this instance, the malformed packets included fragments of valid network management packets that are typically generated. Each malformed packet shared four attributes that contributed to the outage: 1) a broadcast destination address, meaning that the packet was directed to be sent to all connected devices; 2) a valid header and valid checksum; 3) no expiration time, meaning that the packet would not be dropped for being created too long ago; and 4) a size larger than 64 bytes.*

The switching module sent these malformed packets “as network management instructions to a line module,” and the packets “were delivered to all connected nodes,” the FCC said. Each node that received the packet then “retransmitted the packet to all its connected nodes.”

The report continued:

> *Each connected node continued to retransmit the malformed packets across the proprietary management channel to each node with which it connected because the packets appeared valid and did not have an expiration time. This process repeated indefinitely.*
>
> *The exponentially increasing transmittal of malformed packets resulted in a never-ending feedback loop that consumed processing power in the affected nodes, which in turn disrupted the ability of the nodes to maintain internal synchronization. Specifically, instructions to output line modules would lose synchronization when instructions were sent to a pair of line modules, but only one line module actually received the message. Without this internal synchronization, the nodes' capacity to route and transmit data failed. As these nodes failed, the result was multiple outages across CenturyLink's network.*

Restoration and changes for the future

CenturyLink became aware of the outage at 3:56am ET, and by mid-morning it had "dispatched network engineers to Omaha, Neb., and Kansas City, Mo., to log in to affected nodes directly." They traced the problem back to the Denver node. At 9:02pm, the company "identified and removed the module that had generated the malformed packets."

But the outage continued because "the malformed packets continued to replicate and transit the network, generating more packets as they echoed from node to node," the FCC wrote. Just after midnight, at least 20 hours after the problem began, CenturyLink engineers "began instructing nodes to no longer acknowledge the malformed packets." They also "disabled the proprietary management channel, preventing it from further transmitting the malformed packets."

“Much of the network” was functioning normally by 5:07am ET on December 28, but not all nodes were restored until 11:36pm that night.

Even after all nodes were restored, “some customers experienced residual effects of the outage as CenturyLink continued to reset affected line modules and replace line modules that failed to reset,” the FCC said. CenturyLink determined that the network had “stabilized” by 12:01pm on December 29.

Best practices not followed

The FCC report said that several best practices could have prevented the outage or lessened its negative effects. For example, the FCC said that CenturyLink and other network operators should disable system features that are not in use.

“In this case, the proprietary management channel was enabled by default so that it could be used if needed,” the FCC wrote. “While CenturyLink did not intend to use the feature, CenturyLink left it unconfigured and enabled. Leaving the channel enabled created a vulnerability in the network that, in this case, contributed to the outage by allowing malformed packets to be continually rebroadcast across the network.”

The report also said that CenturyLink could have used stronger filtering to prevent the malformed packets from propagating. CenturyLink used filters “designed to only mitigate specific risks.” Instead, CenturyLink could have used “catch-all filters” that only allow expected traffic.

CenturyLink also should have set up “memory and processor utilization alarms” in its network monitoring, the FCC said. Even though the malformed packets “quickly overwhelmed the processing capacity of the nodes,” this “did not trigger” any alarms in CenturyLink’s system.

After the incident, CenturyLink "replaced the faulty switching module and shipped it to Infinera to perform a forensic analysis," the FCC wrote. Infinera engineers still haven't been able to replicate the problem, but the companies "have taken additional steps to prevent a repeat of this particular outage," the FCC said.

Those additional steps include CenturyLink disabling the proprietary management channel. "Infinera has disabled the channel on new nodes for CenturyLink's network and has updated the node's product manual to recommend disabling the channel if it is to remain unused," the FCC said.

The report continued:

> *The service provider and vendor also established a network monitoring plan for network management events to detect similar events more quickly. Currently, CenturyLink is in the process of updating its nodes' Ethernet policer to reduce the chance of the transmission of a malformed packet in the future. The improved Ethernet policer quickly identifies and terminates invalid packets, preventing propagation into the network. This work is expected to be complete in fall 2019.*

When contacted by Ars today, CenturyLink said that the "outage was caused by a network management card that generated malformed packets that unfortunately were retransmitted across parts of CenturyLink's transport network."

CenturyLink further said that it "has taken a variety of steps to help prevent the issue from reoccurring, including disabling the communication channel these malformed packets traversed during the event and enhancing network monitoring. We value our customers and regret any inconvenience this event may have caused."

Impact on Comcast, Verizon, and more

The outage had “rippling effects” on other providers that rely on CenturyLink’s long-haul transport network, the FCC said.

“The outage potentially affected 3,552,495 of Comcast’s VoIP customers for 49 hours and 32 minutes,” with Comcast phone customers potentially experiencing “a fast-busy signal or diminished call quality if calls were transmitted over affected transport facilities,” the FCC said.

The outage also disrupted Comcast’s ability to route 911 calls in Idaho.

Verizon uses CenturyLink’s network to transport portions of its wireless network traffic, and the “outage affected Verizon Wireless’s network across several Western states, including intermittent service problems in one county in Arizona, 12 counties in Montana, 21 counties in New Mexico, and four counties in Wyoming,” the FCC said.

“In Arizona and New Mexico, this outage potentially affected 314,883 users of Verizon Wireless’ network and resulted in 12,838,697 blocked calls (based on historical data),” the FCC said.

Tens of thousands of Verizon customers on Verizon’s CDMA network would have been unable to dial 911 during the outage, the FCC said. 911 service on Verizon LTE was unaffected “because the LTE network does not use the affected CenturyLink network for transport,” the FCC said.

The CenturyLink outage also had major impacts on TeleCommunication Systems (a 911 provider), Transaction Network Services (which provides SS7 service for TeleCommunication Systems and other small network providers), General Dynamics Information Technology (a 911 provider), and

West Safety Services (another 911 provider).

“The CenturyLink outage also had smaller effects on other service providers,” the FCC said. These smaller effects had an impact on millions of people, though. The FCC wrote:

> *AT&T estimates that 1,778,250 users may have been affected. Some of the potential effects include dropped calls, voice service degradation, and callers receiving fast-busy signals when calling. TDS reported that 1,114 of its wireline users may have been affected. 911 call delivery was also affected for several service providers. Bluegrass Cellular, in Kentucky, reported that the outage potentially affected 911 call delivery for 195,384 wireless users. Cellcom, a Wisconsin-based wireless provider, notified the Commission that 53 calls to 911 were transmitted without ANI [Automatic Number Identification] and ALI [Automatic Location Identification]. Cox reported that the outage potentially affected 654,452 VoIP users. In Iowa, US Cellular reported that the outage potentially affected ALI for 911 calls for 94,380 of its wireless users. None of the providers or PSAPs [public-safety answering points] reported any harms to life or property due to the outage.*

https://arstechnica.com/?p=1554119