Level 3 Nationwide Outage
October 4, 2016

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU
CYBERSECURITY AND COMMUNICATIONS RELIABILITY DIVISION STAFF REPORT

MARCH 13, 2018

1. EXECUTIVE SUMMARY

On October 4, 2016, Level 3 Communications (Level 3) experienced a major outage within its network.[1] This outage, the largest reported in the Federal Communications Commission's (FCC or Commission) Network Outage Reporting System (NORS), had a nationwide impact.[2] Approximately 111 million calls were blocked because of the outage, over 109 million of which were on Level 3's interconnected Voice over Internet Protocol (VoIP) networks. Calls to 911 from 15 telephone numbers were blocked, and 117 public safety answering points (PSAPs) nationwide were unable to receive location information for callers. The outage, which lasted for nearly an hour and a half, revealed underlying issues in Level 3's network management practices. The Public Safety and Homeland Security Bureau (PSHSB or Bureau) launched an investigation into the causes, effects and implications of this outage.

As described in greater detail below, the outage occurred when, as part of Level 3's anti-fraud operations, a technician created an improper entry in Level 3's network management software by leaving a number field blank that would normally contain a target telephone number. The network management software interpreted the blank field as an instruction to block all calls, and accordingly blocked all calls across Level 3's network, rather than blocking only those calls from numbers associated with potentially malicious activity. Within four minutes of the beginning of the outage, Level 3's network began sending traffic management alerts indicating a network issue. Once Level 3 and its vendor discovered and addressed this issue, the outage ended. Level 3 has since taken corrective actions that the Bureau assesses should help prevent such outages from occurring in the future.

2. ROOT CAUSE

The Level 3 outage began at 10:06 AM Eastern Daylight Time (EDT) on October 4, 2016. PSHSB's Cybersecurity and Communications Reliability Division (CCR) received NORS reports from 13 different companies regarding this event. CCR staff subsequently spoke with Level 3 and with carriers that experienced significant impact on their networks.

As part of its regular network maintenance practices, which involve network changes once or twice a day, a technician made changes to Level 3's network management software, which manages soft switches and gateways. Specifically, the outage occurred while the technician was conducting routine anti-fraud operations in Level 3's vendor-supplied network management software. The anti-fraud operations were intended to block calls originating from telephone numbers that are not native to Level 3's network that are suspected of association with malicious activity. The technician left empty a field that would normally contain a target telephone number. The network management software interpreted the empty field as a "wildcard," meaning that the software understood the blank field as an instruction to block all calls, instead of as a null entry. This caused the switch to block calls from every number in Level 3's non-native telephone number database.

However, Level 3 has systems to provide alerts when the network is not performing as expected, regardless of cause. Within four minutes of the beginning of the outage, Level 3's network began sending

[1] Level 3 is a global communications provider that provides communications services to enterprise, government and carrier customers.

[2] NORS is the Commission's web-based filing system through which communications providers covered by the Part 4 outage reporting rules must submit reports to the Commission. These reports are presumed confidential to protect sensitive and proprietary information about communications networks. *See* 47 CFR § 4.2.

traffic management alerts to its Network Operations Center (NOC), indicating that nodes were exceeding the appropriate calls per second threshold, which likely happened because blocked callers redialed after failed calls. Level 3 immediately began working to identify and fix the outage. At 11:31 AM EDT, Level 3 and the network management software vendor made a configuration adjustment to correct this issue, and immediately restored inbound and outbound call flows for all customers.

The technician was unaware of the consequences of leaving a field in the network management software blank. Level 3 personnel had not previously observed or experienced this behavior in their network management software. According to Level 3, this was the first time that anti-fraud operations in network equipment caused an outage.

3. NETWORK IMPACT

The outage lasted for one hour and 24 minutes, and affected approximately 29.4 million interconnected VoIP users and approximately 2.3 million wireless users. Approximately 111 million calls were blocked because of the outage, over 109 million of which were on Level 3's interconnected VoIP and wireless networks. This nationwide outage was the largest ever reported in NORS.

In addition, 911 calls to 117 PSAPs were re-routed to West's back-up call center, also known as its Emergency Call Routing Center (ECRC), and were delivered to PSAPs without location information. The call center became overloaded in some instances, and did not complete 911 calls from 15 telephone numbers.

As described below, PSHSB staff contacted several affected service providers to ascertain the effects of the outage outside of Level 3's network, and to evaluate the sufficiency of actions taken in response to the outage.[3]

Verizon Business

Verizon Business's (VZB) alarms notified VZB of the call blocking event at approximately 10:10 AM EDT on October 4, 2016. At that point, VZB began exploring the possibility of re-routing all of its calls around Level 3. VZB contacted Level 3 by 10:47 AM EDT; prior attempts to contact Level 3 were unsuccessful because Level 3's call center was unavailable. Level 3 advised VZB that Level 3 was working with its vendor to restore service. At that point, VZB decided not to initiate any re-routing of its calls because such an effort would take considerable time and VZB determined the outage would be resolved before it could successfully implement call re-routing. VZB initially reported a preliminary estimate of nearly 20 million blocked calls, but later revised its report after analyzing the data to reflect 1.7 million blocked calls in addition to the 109 million blocked calls reported by Level 3. None of the blocked calls on Verizon's network were 911 calls.

West Safety Services

Some of the 911 services provided by West Safety Services (West) rely on Level 3 to route and deliver 911 calls and pseudo Automatic Numbering Information (pANI) to the 911 Selective Router. pANI

[3] The service providers listed do not reflect an exhaustive list of those affected by the outage. PSHSB staff spoke with those carriers experiencing significant impacts on their networks and which acted to minimize those impacts.

allows the switch to send the call to the correct PSAP by providing caller location information. At 10:07 AM EDT, moments after the Level 3 outage occurred, alarms notified West of the outage. West reported that 117 PSAPs nationwide were unable to receive location information for callers. At that point, West began re-routing calls that would otherwise be directed to Level 3. West processed all voice calls in accordance with the interconnected VoIP service providers' or the wireless carriers' pre-defined default routing plans. Where these service providers and carriers use West services as their default route, West's Emergency Call Routing Center (ECRC), or backup call center, re-routed and responded to the calls. The call center then contacted the appropriate PSAP for each of the 911 calls. During the outage, West reported that it re-routed a total of 153 unique 911 calls to the call center.

Level 3 personnel initiated a telephone call to discuss the effects of the outage with West personnel at approximately 10:40 AM EDT. Level 3 and West personnel also communicated about the outage prior to that call, but did not record the times of those earlier calls. At approximately 11:30 AM EDT, West reported that Level 3 had resolved the outage and that West's network was processing all calls normally.

Bandwidth

Bandwidth is a 911 service provider that routes 911 calls through Level 3. Bandwidth has two redundant routes to Level 3, both of which were affected. Bandwidth reported that at 10:13 AM EDT on October 4, 2016, it began experiencing 911 call failures on all calls that were handed off to Level 3 for completion to Selective Routers, or special 911 switches. At 11:31 AM EDT, Bandwidth observed that Level 3 appeared to be processing 911 calls successfully again.

During that time period, Bandwidth automatically re-routed all calls that failed to complete via Level 3 to Bandwidth's emergency call center. However, due to the increase in call volume from Bandwidth and other affected stakeholders, the call center was unable to handle the volume of unexpected calls. During the event, Bandwidth reported that 277 calls to 911 were re-routed to its emergency call center. Of these calls, the only 911 calls that were blocked came from 15 unique originating telephone numbers.

Alarms in Bandwidth's NOC notified the company of the outage. Bandwidth opened a trouble ticket with Level 3 via a web portal, and escalated through multiple channels with Level 3 operations and executives. Other than the use of the Level 3 ticketing systems and escalation procedures to communicate about the outage impacts to Bandwidth, no additional telephone calls or e-mails were exchanged between the parties' respective NOCs during this outage.

4. CORRECTIVE ACTIONS TAKEN BY LEVEL 3 TO PREVENT RECURRENCE

This outage points out several flaws in Level 3's use of its vendor-supplied network management software. Level 3 has taken corrective actions that PSHSB assesses should help prevent such outages from occurring in the future:

1. Level 3 now requires anti-fraud personnel and other personnel that implement targeted switch translations to utilize a network provisioning system instead of implementing those translations directly into the management software. Unlike the foregoing network management software, the new network provisioning system will allow Level 3 to implement anti-fraud measures without affecting live traffic. Level 3 has designed the network provisioning system with guardrails to prevent the kind of error that led to the October 4, 2016 outage.
2. Level 3 audited access to switch management software, the network provisioning system, and all other voice provisioning systems, to ensure that Level 3 personnel have appropriate levels of

access to those systems. This audit resulted in the removal of over 800 accounts across all systems.[4]

These actions are in general accordance with three best practices recommended by the Communications Security, Reliability and Interoperability Council and adopted in 2011:[5]

1. Best Practice 9-7-0588: Network Operators, Service Providers and Equipment Suppliers should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture. Training should be provided for personnel involved in the direct operation, maintenance, provisioning, security and support of network elements.[6]
2. Best Practice 9-7-0589: Network Operators, Service Providers, and Equipment Suppliers should establish a minimum set of work experience and training courses which must be completed before personnel may be assigned to perform maintenance activities on production network elements, especially when new technology is introduced in the network.[7]
3. Best Practice 9-8-8098: Service Providers, Network Operators, and Equipment Suppliers should have policies on changes to and removal of access privileges upon staff member status changes.[8]

[4] Not every account represented a unique or active user.

[5] CSRIC is a federal advisory committee charged with providing recommendations to the Commission to promote the security, reliability and resiliency of communications systems, and is subject to the requirements of the Federal Advisory Committee Act (FACA). *See* 5 U.S.C.A § 10.

[6] Communications Security, Reliability and Interoperability Council, Best Practice 9-7-0588 (2011), *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=9-7-0588.

[7] Communications Security, Reliability and Interoperability Council, Best Practice 9-7-0589 (2011), *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=9-7-0589.

[8] Communications Security, Reliability and Interoperability Council, Best Practice 9-8-8098 (2011), *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=9-8-8098.