Incident Report for Content Switch Denial of Service Attack

October 1, 2012

Issue

On Sunday, Sept. 23, 2012, at 7:16 a.m., the Office of Information Technology (OIT) began receiving automatic notifications from our monitoring systems and from clients that some on-campus web pages, virtual private network (VPN) access, Secure Shell (SSH) access and OIT Private Cloud services were unavailable. Off-campus Internet connectivity for some on-campus customers was also sporadic. The problem was intermittent and did not affect all campus network users.

Background

OIT uses content switches to balance load to multiple servers and to insure availability of a service even in the face of a failure of one or more servers in a cluster behind the content switch. OIT uses multiple content switches to meet the needs of our customers.

Cause

One of OIT's content switches was compromised (analysis of the traffic suggests that this was done from China), and at 7:00 a.m. on Sunday, Sept. 23, it started sending large numbers of packets to a few targeted sites on the Internet. This high load contributed to poor service through the router that serves many of the services hosted at the Computing Center, causing intermittent outages for the on-campus web pages, VPN access, SSH access and OIT Private Cloud services. It also caused one of the multiple processing units in the campus border router to fail, resulting in sporadic off-campus Internet access.

Solution

Once the source of the denial–of-service (DoS) attack was determined to be the content switch, a case was opened with the vendor. A vulnerability in the operating system was recently identified but was believed to be mitigated by other technical measures. The problem was initially resolved on Sept. 23, 2012, at 10:30 a.m. As part of addressing the ongoing problem, we blocked traffic headed toward the most predominant DoS targeted sites. The border router was re-booted to clear the affected processor, and the patch provided by the vendor was applied to the compromised content switch. That patch was later applied to all OIT content switches supplied by the specific vendor.

What Can Be Done to Prevent This Again?

OIT is working with the vendor manufacturer to install an upgraded software package that also includes the patch. In addition, OIT is updating vulnerability management processes to more thoroughly test technical measures used to mitigate vulnerabilities.

Report prepared by:

Raymond Baum
Associate Director
OIT Network Engineering and Operations
University of Colorado Boulder