

Table of Contents

Cisco Security Notice: Response to BugTraq – Cisco IOS Software and NMAP DoS.....1
Revision 1.0.....1
Last Updated 1999 September 23.....1
Please provide your feedback on this document.....1
Summary.....1
Details.....1
Cisco Security Procedures.....6

Cisco Security Notice: Response to BugTraq – Cisco IOS Software and NMAP DoS

Revision 1.0

Last Updated 1999 September 23

Please provide your feedback on this document.

Summary
Details
Cisco Security Procedures

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report: <http://www.securityfocus.com/archive/1/25906> . Cisco responded with the following two statements, which are also archived at <http://www.securityfocus.com/archive/1/27496> and <http://www.securityfocus.com/archive/1/28601> .

```
To: BugTraq
Subject: Re: Cisco and Nmap Dos
Date: Sep 15 1999 8:05PM
Author: Lisa Napier <lnapier cisco com>
Message-ID: <4.2.0.58.19990915190347.00c30c90@twoguys>
In-Reply-To: <4.2.0.58.19990907185808.00be2420@twoguys>
```

Hi all,

An update to this issue: we have been able to reproduce the problem in our labs, but only under specific conditions. At this point, the customer has not been able to confirm or deny the configuration items in effect during this problem.

Essentially what we found was that if fast switching was in use, and if there are multiple equal cost routes for the same destination, the router will install host routes for each destination to ensure load balancing across equal cost paths.

Under these conditions, scanning an entire class A network will use up all of the routers memory in short order.

To avoid this problem, I would recommend using CEF (Cisco Express Forwarding) which handles equal cost paths differently, and more

efficiently than the fast switching model detailed above. CEF is available in IOS version 12.0 for most platforms.

Thank you,

Lisa Napier
Product Security Incident Response Team
Cisco Systems

At 07:12 PM 9/7/1999 -0700, Lisa Napier wrote:

>Hi all,
>
>Sorry for the delay in response.
>
>At first glance, I had thought that this security advisory may have had
>something to do with this issue.
>
><http://cco/warp/customer/770/iossyslog-pub.shtml>
>
>This details a specific issue with the routers response to an invalid UDP
>packet to the syslog port, however your report details strictly ICMP scan
>and tcp port scans.
>
>In speaking with the engineer who is working the case, he was unable to
>view the issue 'live'; the people running NMAP had turned it off, just as
>he had logged into your network, and functionality was pretty much restored.
>
>We have not yet been able to reproduce the problem in house, but are
>still working on it.
>
>The customer support engineer working the case is trying to cause the
>problems you saw with the scan parameters that you specified, in that it
>was only scanning hosts that responded to a ping. If we presume that the
>scan was actually attempting to scan an entire class A network, then the
>behavior seen of maxing out the input queues and therefore memory
>resources is an expected and nasty side effect, and we have indeed seen
>that behavior.
>
>Cisco's product security incident response team is monitoring the case at
>this point, and expecting an update within the next few days.
>
>For those on the list unaware of us, the Cisco PSIRT is the best point of
>contact for reporting a security issue with any Cisco product. The URL
>below gives more details on the Cisco PSIRT.
>
>Thanks,
>
>Lisa Napier
>Product Security Incident Response Team
>Cisco Systems
>
>408 527-8747
>
>http://www.cisco.com/warp/public/707/sec_incident_response.shtml
>
>
>At 05:02 PM 8/31/1999 -0700, Lancashire, Andrew wrote:
> >I don't know if you've ever seen this before. We ran nmap with ICMP
> >discover and standard tcp scan. We ran the scan against the entire 10.0.0.0
> >network range. Although we were only looking for 2 ports, we found that the
> >RSM in our 5500 series (our default route) was running out of memory and
> >had to be rebooted by our Network Services group multiple times in the 18
> >hour stretch it took to complete. One of the interesting things is that we

> >were only generating about 3-5 Mbs and the 5500 can pass Gigabits. I have
> >not heard of this problem before. We contacted Cisco and sent them the
> >details. Below is the response to one of our engineers.
> >
> >Andrew
> >
> >-----Original Message-----
> >From: khollis [SMTP:khollis cisco com]
> >Sent: Tuesday, August 31, 1999 7:59 AM
> >To: wescotd sutterhealth org
> >Subject: Regarding Case Number V44290
> >
> >Hi Dave, as I recall, the symptom we had to work/troubleshoot with was the
> >router consumed lots of memory. Never heard about packets being dropped. So
> >it seems like we forwarded everything nmap sent to us. The thing to keep in
> >mind is that the router will dynamically allocate memory as necessary so
> >that it can keep up with the load provided to it. Although we did not know
> >nmap was running at the time, we noticed the memory consumed by the IP Input
> >process dropped from 40M+ to an acceptable level of (4-5M) after nmap was
> >shut down. This proves that the router need this much memory to process the
> >entire load generated by nmap.
> >
> >I suspect nmap was doing much more than you've been able to calculate. It's
> >obvious that running nmap continuously for 18-19 hours caused this problem.
> >One possible explanation is constantly flooding the router w/64 byte
> >packets for this timeframe could have caused the router's memory to become
> >seriously fragmented. Also, I guess we can't tell, but another question
> >would be how many tcp sessions were requested/open on the router after this
> >timeframe?
> >
> >Port scanners have a reputation of helping identify potential security
> >problems. However, they are also known to cause problems...
> >
> >Hope this helps,
> >KennyH.

To: BugTraq
Subject: Re: Nmap and Cisco Dos, clarification --
Date: Sep 23 1999 6:30PM
Author: Lisa Napier <lnapier cisco com>
Message-ID: <4.2.0.58.19990923171636.00c83a90@twoguys>
In-Reply-To: <E96A622162DED211831F0008C75DDD7B011BB5AC@gpscldx.sutterhea lth.org>

Hi Andrew,

The message you are quoting from me was my attempt to refute the possible causes suggested by another poster, not as a suggestion for the reasoning behind the nmap problem. I was attempting to indicate that I did not think that ARP was the problem, but was waiting for further testing and details, which I did not have at the time.

Apologies, as I was not clear in my message. I believe my later follow up message of 9/15/99 is exactly in-line with what Kenny had tested in house.

Just further clarification.

Thank you,

Lisa Napier
Product Security Incident Response Team
Cisco Systems

At 01:44 PM 9/22/1999 -0700, Lancashire, Andrew wrote:

>This is to clarify what is being put out by Cisco and what we are being told
>by Cisco.
>
>Two e-mails below is what Cisco is telling us and makes allot more sense
>than what Cisco is telling Bugtraq. The last post to Bugtraq made mention
>that the arp cache was filling up and allocating memory for both reachable
>hosts and unreachable hosts (incompletes). Although what Lisa describes is
>>true regarding the arp cache, it would not be true for our or most other
>sane persons environment. Since routers will only arp for what is local,
>that would mean that for the arp cache to fill up and us all the memory all
>networks in the 10.x.x.x range would need to be local. So that's not gonna
>happen but if you read the e-mail below that from Kenny (also at Cisco) his
>explanation makes allot more sense considering we have hundreds of routers.
>
>Thank You
>
>Andrew
>
>P.S. Congratulations on the re-opening of PacketStorm
>_____

>
>
>
>Subject: Re: Cisco and Nmap Dos
>To: BUGTRAQ SECURITYFOCUS COM
>
>
>Hi all,
>
>
>I wanted to address the items listed here. We are still investigating this
>problem, and hope to have more information later on in the week.
>
>
>Item 1, OSPF is not an issue. According to the configuration information
>provided to us by the customer, OSPF is not in use.
>
>
>Items 2, 3 & 4. IOS actually handles ARP in the following manner:
>
>
>When we receive a packet destined for something not already in our ARP
>table, we enter an "incomplete" entry in the ARP table. Then we will rate
>limit ARPs to once every 2 seconds to that destination. Any additional
>packets to that same destination will be dropped until the ARP entry is
>completed. This is on a per destination basis.
>
>
>"Incompletes" (ARP requests that have not been responded to) get dropped
>after approximately 1 minute from the last time we sent an ARP request for
>that non existent address.
>
>
>Incomplete entries MAY stay around longer, as the process that is
>responsible for cleaning up the ARP table may not have enough time to
>complete before it is called again, if we have a lot to clean up, which may
>be relevant to this case. The incomplete entries will eventually get
>cleaned up, but it may take two or three minutes, two or three cycles of the
>process that cleans up the table.
>
>
>Under a dedicated, intense nmap scan, a very large number of ARP requests
>may be generated, causing the ARP table to grow very large with "incomplete"
>entries. These entries consume memory. As the amount of free memory
>declines and demand on the processor to handle outstanding packets

>increases, ARP processing falls behind and throughput on the router may
>decline significantly. Once the scan is stopped, processing catches up and
>things return to normal.
>
>
>So, to my knowledge IOS should be doing the right thing, we only queue one
>ARP request at a time, every 2 seconds, until the ARP entry is resolved, we
>rate limit requests, dropping all additional packets, until the ARP entry is
>resolved, and we clean up the outstanding incomplete requests within a few
>minutes.
>
>
>I hope that helps address some of the concerns put forth. Hopefully we will
>have further updates shortly.
>
>
>Thank you,
>
>
>Lisa Napier
>Product Security Incident Response Team
>Cisco Systems
>_____
>_____
>_____

>-----Original Message-----
>From: khollis [SMTP:khollis cisco com]
>Sent: Wednesday, September 15, 1999 11:31 AM
>To: wescotd sutterhealth org
>Subject: Regarding Case Number V44290
>

>Hello Dave, I've done some testing here with Nmap. I was able to create a
>test bed that can cause problems & symptoms similar to those you reported.
>But in summary, the router is functioning normally & depending on the
>network topology the behavior you experienced would be expected.
>
> >From show processor memory, the ip input process is the process that
>maintains the ip fast switching cache. This fast switching cache is used
>when forwarding packets to avoid interrupting the cpu for repetitive route
>table lookups. The key issue is the behavior of the fast cache and the way
>it gets built.
>
>
>There are a number of scenarios that will cause the fast cache to install an
>entry that essentially looks like a host route. For instance, with only 1
>path to a destination, we will install an entry into the fast cache that
>covers the entire network. Example: 100.0.0.0/8. However, when multiple
>equal cost paths to a destination exist, we will install an entry into the
>fast cache for each destination. Example: 100.0.0.1/32, 100.1.1.1/32,
>100.2.2.2/32...and so on. This helps ensure load balancing. Additionally,
>depending on whether routes are directly connected, and/or subnetted, or the
>next hop of a static route, the results can vary.
>
>
>When running Nmap & scanning every address in a class A ip network, if
>conditions warrant the installation of a /32 entry into the fast cache this
>would allow the fast cache to consume a tremendous amount of memory and in
>that scenario all available dram could be consumed. This creates additional
>problems because there isn't enough memory to support other features on the
>router.
>
>
>Since Nmap isn't a normal application ran on networks, this issue isn't a
>concern in most networking environments. However, if this is a major concern
>you could run CEF (Cisco Express Forwarding). The behavior I just explained
>does not occur when running CEF. But you will need to run 12.0 on the Cat5

```
>RSM. Other workarounds such as disabling fast switching (no ip route-cache)
>or using max-paths 1 aren't really feasible. CEF is the better solution.
>
>Thanks,
>KennyH.
>
>_____
```

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/warp/public/707/sec_incident_response.shtml. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.