Global Information Assurance Certification Paper

Cisco IOS Vulnerability results in unexpected reload
James Born
Version 1.2d

The Vulnerability

Cisco released a security advisory, May 24, 2001 describing a vulnerability of its Cisco IOS Software, Cisco Bug ID CSCds 07326, reporting that "security scanning software can cause a memory error in Cisco IOS versions 12.1(2)T and 12.1(3)T that will cause a reload to occur". This vulnerability can cause service interruptions and could be exploited as a denial of service attack; cisco advises customers using the affected IOS releases to upgrade their software immediately. http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml. This vulnerability is significant because the reload can be caused by an unauthorized person as well as by an authorized network administrator testing the network.

Background

Identifying network device types, their software and versions, IP addresses, etc. are the first steps a hacker takes to look for vulnerabilities to exploit and gain unauthorized access to private information resources. This "footprinting" process can be followed by network scanning directed at revealed targets with tools like **traceroute** (UNIX), **tracrt** (WinNT), or with scanning software like **netcat** http://www.l0pht.com/~weld/netcat/ and **nmap** http://www.insecure.org/nmap. The search for vulnerable devices commonly begin with routers, because traceroute output often terminates at a network border router or firewall, giving the hacker an initial target as well as a hint of the victim network sitting behind the router.

Scanning with the above mentioned utilities can reveal the IP address of the router, what ports are open on the router and at times, what the device make/model is. Knowing what the vendor make/model is, for instance a Cisco 2600 router, gives a hacker enough information to pursue an attack on this device based simply on the latest technical advisory regarding known vulnerabilities of that system. Even the most conscientious network administrators that read the latest security alert as it is posted can still be beaten by a determined hacker that has targeted their system and who attacks before the patch can be applied.

For instance, a router might be identified as a Cisco router from its characteristic response to a particular tcp-connect attempt. Upon scanning Cisco finger service and virtual terminal ports 2001, 4001, 6001 the Vty's respond back with **finger –l @<host>**, a response particular to a Cisco device. Connecting to port 4001 via a web browser would give results like **User Access Verification Password: Password: Password: % Bad passwords,** again a Cisco characteristic response (Hacking Exposed, pp. 429-430). These are examples of informational searches, which set the stage of an attack, next come the mapping and/or entry into the network.

Upon finding an open port a hacker might take advantage of, for example, the snmp read-write ILMI community string vulnerability, http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml. Using the **snmpwalk** command on a vulnerable device will reveal the snmp objects **sysName** = router hostname, **sysContact** = administrator contact name and phone number as well as the **sysLocation** = physical location of the device. These and other objects can be changed possibly resulting in a loss of ATM service not to mention the fact that these ports are vulnerable to an SNMP packet flood resulting in a denial of service attack. An alarming observation regarding SNMP security is made by the authors of Hacking Exposed, p.430, which states, "…that in many organizations, SNMP is all but forgotten about during security reviews. Perhaps it's because SNMP runs over UDP (a commonly missed portion of the protocol stack), or maybe few administrators know about its function. Either way, SNMP can be (and usually is) missed in security reviews, leaving gaping holes for attack".

The Cisco IOS Bug

This latest Cisco alert describes an operating system flaw that hackers can exploit but with a twist since, the service interruption can also be initiated by the network's own protectors. Security scanning software used to investigate known vulnerabilities of various open ports attempts to make a TCP connection to ports 3100-3999, 5100-5999, 7100-7999, and 10100-10999. Cisco IOS software cannot be configured for services supporting these ports nor to accept connection attempt to these ports. Attempts to connect to these ports will cause a memory corruption in the affected IOS releases which will cause the router to unexpectedly reload the next time the configuration file is accessed, for example as when the **show running-configuration** or **write memory** commands are executed. One indicator of the scanned software-related crashes found on equipment logs was the **attempt to connect to RSHELL** error message. Cisco stated that while this bug can be used to mount a denial of service (DoS) attack "this defect by itself does not cause the disclosure of confidential information nor allow unauthorized access". At the time this article was written the problem had not been reported to Cisco as having been used as a hacker exploit although unexpected device reboots were reported from Cisco customers following the use of scanning software. (http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml.)

Devices which use the Cisco IOS:

The Cisco Security Advisory lists products that use the Cisco Internetwork Operating System Software (IOS) and explains that to determine if your device is running it you should type the **show version** command. Cisco IOS software will respond with "IOS" or "Internetwork Operating System Software" while other Cisco devices not running this software will either not have the **show version** command, or will respond with different output. Below is a list of commonly used Cisco products that run the IOS software but this is not a complete list, you should issue the show version command or call Cisco for information about your Cisco product.

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS,RSM, 8xx,ubr9xx,1xxx, 25xx, 26xx, 30xx, 36xx, 38xx, 40xx, 45xx, 47xx, AS52xx,
- AS53xx, AS58xx, 64xx, 70xx, 72xx (including the ubr72xx), 75xx, and 12xxx series.
- Most recent versions of the LS1010 ATM switch.
- Some versions of the Catalyst 2900XL LAN switch.
- The Cisco DistributedDirector.

Software fixes listed by version

Upgrade your affect IOS versions according to the table below. The Advisory provides a list of affected IOS versions and their respective upgrades but some have multiple releases, Cisco suggests using the Maintenance release as soon as it becomes available.

> Interim = less testing than maintenance release, only use if maintenance unavailable, then upgrade as soon as it becomes available.
>
> Maintenance = most heavily tested and recommended release by cisco.

Affected version	Interim release	Maintenance release
12.1DB	none	12.1(4)DB
12.1DC	none	12.1(4)DC
12.1T	12.1(4.3)T	12.1(5)T
12.1XB	none	12.2(1)
12.1XC	none	12.2(1)
12.1XE	none	12.2(1)
12.1XF	none	12.2(1)
12.1XG	none	12.2T*
12.1XH	none	12.2(1)
12.1XI	none	12.2(1)
12.1XJ	none	12.2T*

12.1XK	none	12.2(1)
12.1XL	none	12.2(1)
12.1XP	none	12.2T*
12.1XQ	none	12.2T*
12.1XS	none	12.1(5)XS
12.1XT	none	12.2T*

* Cisco states that this release does not have a rebuild solution therefore you should upgrade to 12.2T when it becomes available.

Significance

This vulnerability can result in an unexpected network outage which can be service affecting depending on the redundancy and configuration of your network.

In addition to the exploits mentioned above, this latest Cisco bug is signified by the fact that a service outage could be inadvertently caused following the network's administrator's or consultant's security scan. Imagine a dedicated engineer that has convinced his superiors to pay for a security penetration check of the company network. They sign off on or initiate scanning as a part of the test for known port vulnerabilities but soon after such scans begin and/or possibly not until the scans are completed the network crashes. The engineer is positive that they did not bring down the network therefore they begin a forensic examination to get to the root of the problem. After checking the circuits and later the device logs and they should eventually come across this technical advisory and fix. However, explaining how you brought down your company's network and why you did not know it could be a "resume generating" event, illustrating the importance of addressing exactly how security scanning and software updates are implemented for the company.

Having a thorough security policy and written permission to scan is critical insurance to address such unforeseen issues. The SANS web site is an excellent starting point to find information and resources regarding security policies http://www.sans.org/newlook/resources/policies/policies.htm. Here you can learn the basics of security policy content which can include procedures for acceptable use, remote access, configuration management, data backup/storage, and disaster response to name just a few of the topics covered on this site http://www.sans.org/newlook/resources/policies/bssi3/index.htm
Having proper documentation in place that is implementable and enforceable ensures that the client's needs are being addressed and should free the security engineer of any reservations they might have to act proactively to meet these needs.

Conclusion

The Cisco vulnerability described here is troubling not only for its exploitability to attack but also because the service interruption may as likely originate from an unwitting albeit uninformed administrator. In addition, the outage may not occur during or even soon after the attack making the initial incident analysis more difficult. This situation becomes more complicated if the company's security policy does not address authorized network scanning and if the culprit never secured proper written authorization to conduct the scan in the first place. The take home lesson for the security engineer is to stay informed, keep up to date on the latest vulnerabilities but more importantly to understand the policies in place and to "get it in writing".

References

- Cisco Security Advisory: IOS Reload after Scanning Vulnerability http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml
- Netcat resource http://www.l0pht.com/~weld/netcat/
- Nmap resource http://www.insecure.org/nmap
- Joel Scambray, Stuart McClure, George Kurtz, Hacking Exposed Network Security Secrets & Solutions(second edition), pp. 429-430, Berkeley, Osborne/McGraw-Hill, 2001
- Cisco Security Advisory: Cisco IOS Software SNMP Read-Write ILMI Community String Vulnerability http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml
- SANS Institute, Model Security Policies by Michele Crabb-Guel http://www.sans.org/newlook/resources/policies/policies.htm
- SANS Institute, Model Security Policies Section Three: Policies and Procedures by Michele Crabb-Guel http://www.sans.org/newlook/resources/policies/bssi3/index.htm

Questions

1) Security policies should be
   a. written by a lawyer in legalese
   b. restricted to upper management viewing
   c. consider security issues at all costs
   d. be implementable and enforceable

Security policies should be implementable and enforceable (d); they should be concise, easy to understand and should balance protection with productivity.
http://www.sans.org/newlook/resources/policies/bssi3/index.htm

2) Which Cisco IOS version(s) is/are vulnerable to security software related reboots?
   a. 12.1(2)T and 12.1(3)T
   b. 11.1(2)T and 11.1(3)T
   c. 12.2T and 12.3T
   d. 11.1(3)T and 12.1(3)T

Versions 12.1(2)T and 12.1(3)T are vulnerable (a) as stated in the advisory.
http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml

3) Why is this IOS vulnerability significant to the author?
   a. The outage can be caused by unauthorized activity
   b. The outage can be caused by authorized activity
   c. The outage is unrecoverable
   d. The outage is untraceable

The reboot is caused by a memory error resulting from scanned tcp-connect attempt to certain high ports. Security scanning is used by both authorized and unauthorized users therefore it is significant that the authorized user could unwittingly bring down their own network (b)

4) What type of attack is this?
   a. syn-fin host flood
   b. DDoS
   c. DoS
   d. Smurf

Since the device reboots unexpectedly interrupting service, it can be exploited as a denial of service attack (c).

5) What command brings about the unexpected reboot on affected systems?
   a. show version
   b. show ip interface brief

c. show running configuration
d. show controllers

Issuing any command that accesses the configuration will initiate a reboot to the affected system, such as show running configuration or write memory (c).

6) Are all affected IOS versions rebuildable? T/F

False, the table lists several versions that cannot be rebuilt, for these releases Cisco suggests upgrading to IOS version 12.2T once it is made available.

6) Basic utilities such as traceroute or tracert can be used to "hack" a network? T/F

True, traceroute output often ends at a border router or firewall, giving the hacker a starting point to attack. Fingerprinting the device make and model can be enough information for an attack based upon known vulnerabilities to unpatched systems.

7) Cisco recommends replacing your affected version with the latest Maintenance release? T/F

True, Cisco recommends using the Maintenance release over the Interim release because it is the most heavily tested.

8) This vulnerability exists on all Cisco devices? T/F

False, Cisco lists those commonly used devices affected and also lists many devices that do not use the IOS software and are not affected.
http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml

9) You can determine if your Cisco device runs IOS software by issuing the write memory command? T/F

False, issuing the show version command should result in "IOS" or "Internetwork Operating System" if it is running IOS software, Cisco devices not running this software will either not have the **show version** command, or will respond with different output.

10) Log files can assist in determining a reason for outage on affected systems? T/F

True, one indicator of the scanned software-related crashes found on equipment logs was the **attempt to connect to RSHELL** error message.

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event