



Developments and Trends in Attacks Against Network Devices

FIRST TC, Uruguay, November 2008



Dario Ciccarone

**Incident Manager
Product Security Incident Response Team (PSIRT)
Cisco, Inc.**

Agenda

Cisco PSIRT mission and process

Security in the Press

The Evolving Threat Landscape

The Future, What We're Doing, & What You Should Do

Questions

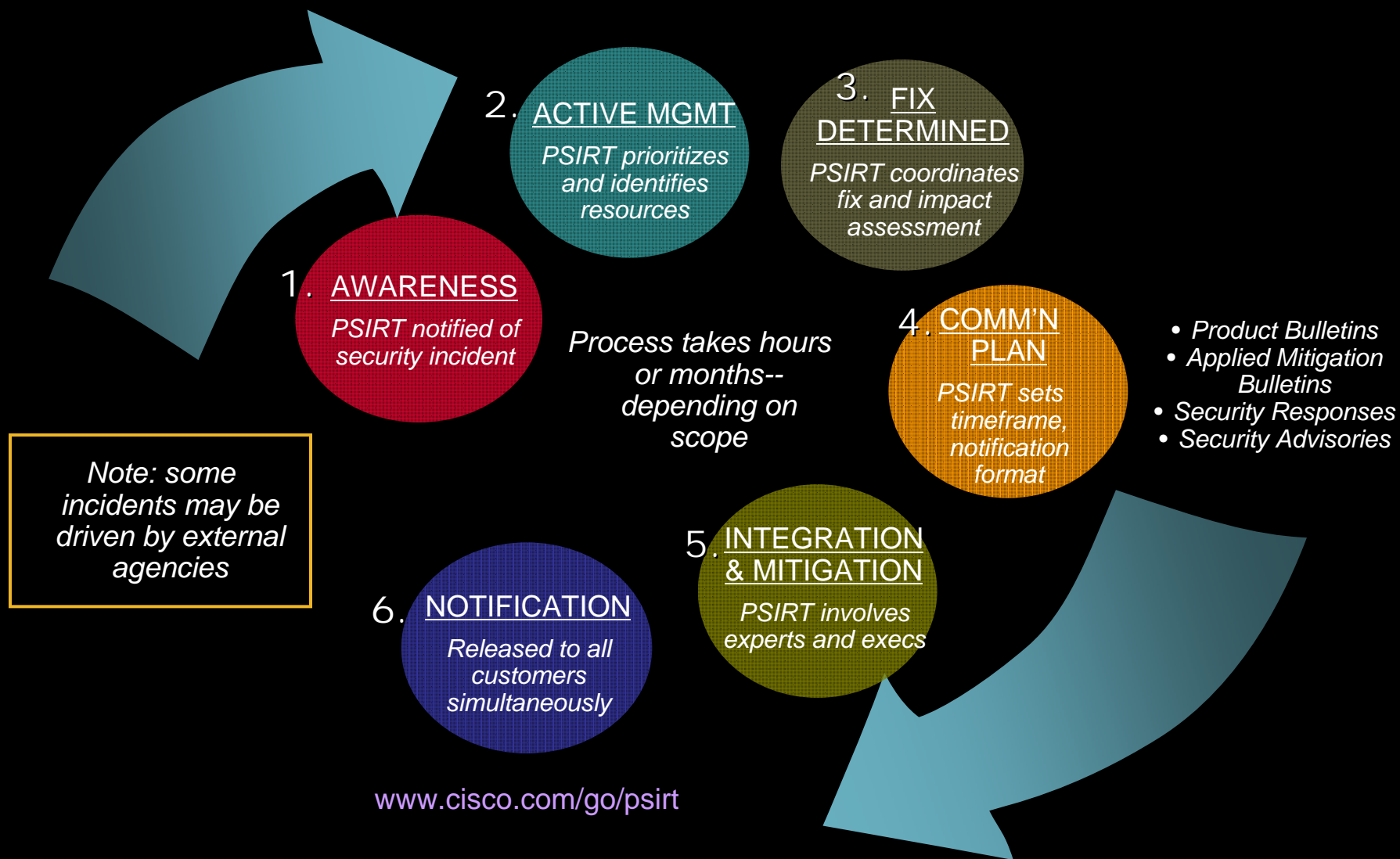


PSIRT Mission

- Global team assisting customers with the ongoing security of their networks through identification, resolution and prevention of vulnerabilities in Cisco products
- Provides specialized, experienced support to handle customer security incidents
- Represents Cisco in the incident response and product security communities
- Single point of contact for receiving and resolving internal and external reports of vulnerabilities in all Cisco products since 1995
- Creates and publishes Cisco Security Advisories and Responses
- Fair public disclosure: everyone notified at the same time
- Escalation support for customer security incidents upon request
- Coordination as required with external agencies (CERT/CC, CPNI, etc.)

www.cisco.com/go/psirt for additional information

Incident Handling Process



Everyone knows about these . . .

Click Here to Install Silverlight United States Change | All Microsoft Sites

Microsoft TechNet

TechNet Home | TechCenters | Downloads | TechNet Program | Subscriptions | Security Bulletins | Archive

Search for

TechNet Security
Security Bulletin Search
Library
Learn
Downloads
Support
Community

TechNet Home > TechNet Security > Bulletins

Microsoft Security Bulletin MS08-067 – Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Dan Kaminsky Reveals DNS Flaw At Black Hat


More than 80 technology vendors launched an unprecedented campaign to fix a flaw in widely distributed DNS software that could allow a form of attack called DNS cache poisoning.

By Thomas Claburn, [InformationWeek](#)
Aug. 6, 2008
URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=209903948>

At the [Black Hat](#) conference in Las Vegas on Wednesday, attendees occupied every available seat and most of the floor space to hear security researcher Dan Kaminsky finally explain the [Domain](#) Name System (DNS) [vulnerability](#) that has been the talk of the Internet security community since early July.

Original URL: http://www.theregister.co.uk/2008/05/13/debian_openssl_bug/

Debian fixes serious crypto bug Locksmith overtime for sys admins



Home > Support > SunSolve >

[Printer-Friendly Page]

Document Audience:	PUBLIC
Document ID:	201391
Old Document ID:	(formerly 102802)
Title:	Security Vulnerability in the in.telnetd(1M) Daemon May Allow Unauthorized Remote Users to Gain Access to a Solaris Host
Copyright Notice:	Copyright © 2008 Sun Microsystems, Inc. All Rights Reserved
Update Date:	Wed Feb 28 00:00:00 MST 2007

Solution Type Sun Alert

Solution 201391: Security Vulnerability in the in.telnetd(1M) Daemon May Allow Unauthorized Remote Users to Gain Access to a Solaris Host

Sun support customers: more support information is available after you sign in.
[Login](#)

The new Member Support Center for SunSpectrum

OpenSSL meant that potentially predictable (before 2006) are potentially vulnerable.

... but what about these ?

The screenshot displays two overlapping web pages. The top page is the Symantec website, featuring a navigation menu with 'Business' selected and a search bar. The main content area shows an article titled 'Drive-By Pharming: How Clicking on a Link Can Cost You Dearly' dated 02-15-2007. The bottom page is the NetworkWorld SecurityBlog, showing a search bar and a post titled 'US-CERT warns of SNMPv3 vulnerability' dated 06/12/2008. The post text describes a flaw in SNMPv3 authentication and mentions a Cisco update. A sidebar on the right of the SecurityBlog lists various security topics and a search bar. A 'CPNI' logo is visible in the top right corner of the Symantec page.

Symantec Confidence in a connected world.

Norton Business Partners | Store | About Symantec

Overview Solutions Products Services Training Support

Emerging

Register | Login

STN Peer-to-Peer Discussion Forums : Security Response Blog : Emerging : Drive-By Pharming

Article Options XML

Drive-By Pharming: How Clicking on a Link Can Cost You Dearly

02-15-2007 12:00 AM Zulfikar Ramzan writes:

I wanted to talk about a recent new attack, called Drive-By Pharming, which I co-authored with Dr. Stamm and Markus Jakobsson of the Indiana University School of Informatics. It is a Web page that, simply when viewed, results in substantive configuration changes to the browser.

NetworkWorld

Home News Research Centers

- Security
 - Anti-Virus / Spyware / Spam
 - Compliance & Regulation
 - Firewalls / VPN / Intrusion
 - NAC
 - Services
 - Cisco Security Watch
 - Microsoft Security Watch
 - LANs & WANs
 - VoIP & Convergence

Log in Post Register

Search Community / blogs: [input] Search

US-CERT warns of SNMPv3 vulnerability

By SecurityBlog on Thu, 06/12/2008 - 4:25am.

A flaw in many implementations of SNMPv3 could be exploited to bypass the authentication mechanism of affected systems. Simply put, attackers could read SNMP packets to find system credentials, then use forged packets to gain access to the system. US-CERT is urging users to check with their vendors for an update.

Cisco has released an update that is [available here](#).

Advertisement:

Google

Systems Affected:

- Google Mini Search Appliance (confirmed)
- Google Search Appliance (possible)

Home Contact us FAQ Glossary Public key Sitemap Cymraeg What's new

CPNI
Centre for the Protection of National Infrastructure

Search: [input] GO

Advanced search

About CPNI

The threats

Security planning

Methods of attack

Protecting your assets

Products and services

- CSIRTUK advisories
 - Advisories archive
- General protective security publications
- InfoSec briefings
- InfoSec technical notes
- InfoSec vulnerability disclosures
- Good practice guidelines

Home > Products and services > CSIRTUK advisories > Advisories archive > April 2005 > NISCC Vulnerability Advisory ICMP - 532967

April 2005

NISCC Vulnerability Advisory ICMP - 532967

ID: 00308
Ref: 1205
Date: 12 April 2005:12:55:23
Version: 1

Title: NISCC Vulnerability Advisory ICMP - 532967

Abstract:

Vendors affected: multiple

Operating systems affected: multiple

Applications affected: multiple

Title
=====
NISCC Vulnerability Advisory ICMP - 532967

Detail
=====
NISCC Vulnerability Advisory 532967/NISCC/ICMP

Vulnerability issues in ICMP packets with TCP payloads


SecurityBlog is written by NetworkWorld Multimedia Editor Jason Meserve

XML feed

SecurityBlog archive.

arch Advisory

Month of bugs anyone?



WIKIPEDIA
The Free Encyclopedia

navigation

- Main page
- Contents
- Featured content
- Current events
- Random article

search

Go Search

interaction

- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

GNUCITIZEN


Information Security Think Tank

Blog Archive About Portfolio Services Training Advertise Contact Home Lab Company Network Search

ROUTER HACKING CHALLENGE

published: February 3rd, 2008


We want you to hack your router! Yes, You. We want you to hack your router and make your findings public on this very same page, the [slackers forum](#) or at [hackerwebzine\[at\]gmail\[dot\]com](mailto:hackerwebzine[at]gmail[dot]com). The best and most interesting hacks will receive credit, a lot of attention and good media coverage.



The challenge is supposed to run from 2nd February until 29th February, though it is something that is yet to be clarified because we know that there is a lot to be found.

The reason why we do this is because we want you to help the community to map the current state of embedded devices vulnerabilities. GNUCITIZEN members **have been actively involved** with finding vulnerabilities in routers in the past. We believe that embedded devices hacking is a huge topic that is yet to be explored in depth. Your submissions will be included in numerous presentations and research materials and will be credited appropriately.

The rules are very flexible, every kind of exploit is allowed. From buffer overflows to CSRF issues that plague many routers.

» more | » comments rss | posted by [pdp](#) | syndication and integration ( ShareThis)

Information Security Services

cutting-edge information security services




GNUCITIZEN Security Training

cutting-edge it security training

» GNUCITIZEN CUTTING-EDGE THINK TANK

» POST YOUR GIGSI IT IS ONLY 100.0 USD FOR 30 DAYS.

GNUCITIZEN PRODUCTS

-  **Blogsecurity** is a division of GNUCITIZEN. The initiative was established to provide social media security services through our free automated testing engine. The Blogsecurity team is also engaged to deliver quality content on issues concerning social media technologies.
-  **Netsecurity** is a division of GNUCITIZEN. The initiative was established to provide network security services through our free automated testing engine. The service is still in private-beta.
-  **Websecurity** is a division of GNUCITIZEN. The initiative was established to provide a fee web application security framework for automated and manual penetration testing. The service is still in private-beta.

create account

orations. The where they're

Explorer, Mozilla

driver bugs;^[3]

the Hardened

[edit]

And multiple vendors “feel the love” 😊

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]

MILWORM

[hardware - remote]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2008-10-31	A-Link WL54AP3 and WL54AP2 CSRF+XSS Vulnerability	1133	R	D	Henri Lindberg
2008-10-14	Telecom Italia Alice Pirelli routers Backdoor from internal LAN/WAN	6837	R	D	saxdax & drpepperONE
2008-09-22	Sagemcom Bus F80ST Remote CSRF Exploit (dhcp hostname attack)	3795	R	D	UnderBnG Crew
2008-09-17	Cisco Router HTTP Administration CSRF Command Execution Exploit	6073	R	D	Jeremy Brown
2008-09-17	Cisco Router HTTP Administration CSRF Command Execution Exploit 2	8537	R	D	Jeremy Brown
2008-09-05	Micro-Tik RouterOS <= 3.13 SNMP write (Set request) PoC	4855	R	D	ShadOS
2008-08-25	Belkin wireless G router + ADSL2 modem Auth Bypass Exploit	6362	R	D	noenser
2008-07-29	Cisco 7940 SIP Phone HTTP Remote Denial of Service Exploit	8866	R	D	Andy Davis
2008-06-2	Linksys WRT54G (Firmware 1.06.9) Security Bypass Vulnerabilities (2)	22120	R	D	meathive
2008-03-20	Linksys WRT54G Firmware 1.06.03 Security Bypass Vulnerabilities	16342	R	D	meathive
2008-03-21	ZyXEL ZyWALL Quagga/Zebra (default pass) Remote Root Vulnerability	8331	R	D	Pranav Joshi
2008-02-18	Thecus N5200Pro NAS Server Control Panel RFI Vulnerability	5089	R	D	Crackers_Child
2008-02-14	Linksys WRT54GL (Firmware <= 1.0.4.000) Multiple Vulnerabilities	6063	R	D	ikki
2008-01-20	Belkin Wireless G Plus MIMO Router F5D9230-4 Auth Bypass Vulnerability	4008	R	D	DarkFig
2007-12-2	Linksys WRT54GL DVR 3204 Logfile Information Disclosure Exploit	3779	R	D	Alex Hernandez
2007-12-18	router YDSL Device (Goahead WEBSERVER) Disclosure Vulnerability	2376	R	D	NeoCoderz
2007-10-11	Apple iPhone/iPhone 1.1.1 BF File Remote Jailbreak Exploit	14649	R	D	Niacin and Dre
2007-02-11	IP3 NetAccess < 4.1.9.6 Remote Arbitrary File Disclosure Vulnerability	4305	R	D	Sebastian Wolfgarten
2007-01-24	PA168 Chipset IP Phones Weak Session Management Exploit	4919	R	D	Adrian "pagvac" Pastor
2006-10-24	Cisco WRT54GL Concentrator <= 4.1.7, 4.7.2 (FTP) Remote Exploit	8894	R	D	prdelka
2006-08-08	Barracuda Spam Firewall <= 3.3.03.053 Remote Code Execution (extra)	7557	R	D	PATz
2006-08-07	Barracuda Spam Firewall <= 3.3.03.053 Remote Code Execution	6041	R	D	Greg Sinclair
2006-07-20	Cisco/Protego CS-MARS < 4.2.1 (JBoss) Remote Code Execution Exploit	6728	R	D	Jon Hart
2006-07-18	BT Voyager 2091 (Wireless ADSL) Multiple Vulnerabilities	6304	R	D	Adrian "pagvac" Pastor
2006-06-08	D-Link Access-Point <= 2.10na (DWL Series) Config Disclosure Vuln	15007	R	D	INTRUDERS
2005-11-20	Google Search Alliance proxystylesheet XSLT Java Code Execution	11546	R	D	H. D. Moore
2005-07-03	Nokia Affix < 3.2.0.1 Http Remote Client Exploit	8791	R	D	Kevin Finisterre
2005-02-19	Thomson 7940 PDS1 Password Validation Exploit	4872	R	D	MurDoK
2004-08-11	D-Link DCS-900 Camera Remote IP Address Changer Exploit	7125	R	D	n/a
2004-07-28	HP Web JetAdmin 6.5 (connectedNodes.ovpl) Remote Root Exploit	6178	R	D	FX
2004-03-28	Multiple Cisco Products Vulnerabilities Exploit (Cisco Global Exploiter)	7304	R	D	Link Angels
2003-08-10	Cisco IOS 12.0/11.x HTTP Remote Integer Overflow Exploit	8485	R	D	FX
2001-01-19	Cisco Password Bruteforcer Exploit	11585	R	D	norby

[hardware - dos]

DATE	DESCRIPTION	HITS	R	D	AUTHOR
2008-10-10	Nokia Mini Map Browser (array sort) Silent Crash Vulnerability	1459	R	D	ikki
2008-09-26	Windows Mobile 6.0 Device long name Remote Reboot Exploit	1818	R	D	Julien Bedard
2008-09-14	Nokia e90/n82 (e60v3) Remote Denial of Service Vulnerability	2964	R	D	wins.mallow
2008-09-07	Samsung DVR SHR2040 HTTPD Remote Denial of Service DoS PoC	2545	R	D	Alex Hernandez
2008-08-03	Xerox Phaser 8400 (reboot) Remote Denial of Service Exploit	2738	R	D	crit3rion
2008-02-03	Micro-Tik RouterOS <= 3.2 SNMPd snmp-set Denial of Service Exploit	3941	R	D	ShadOS
2008-01-24	Apple iPhone 1.1.2 Remote Denial of Service Exploit	7612	R	D	c0ntex
2007-12-05	Cisco Phone 7940 Remote Denial of Service Exploit	4894	R	D	MADYNES
2007-09-18	Aircenson N520 HTTPD Remote Preauth DoS / BOF PoC	3903	R	D	Alex Hernandez
2007-08-27	Thomson SIP phone ST 2030 Remote Denial of Service Exploit	2629	R	D	MADYNES
2007-08-21	Cisco IP Phone 7940 (3 SIP messages) Remote Denial of Service Exploit	3733	R	D	MADYNES
2007-08-11	Cisco IP Phone 7940 (3 SIP messages) Remote Denial of Service Exploit	4513	R	D	MADYNES

Cisco

Belkin

And another one

Linksys

Barracuda

Another vendor

Looking back – the interest was always there

----| 2. Introduction

When I think about routers in general, I feel exactly like I do when I go to the supermarket and see all this food and then I can't stop thinking of mad cow disease, CJD, GMO... It makes me feel dizzy. Just go on cisco.com and check what cisco 7500 is used for and how many corporations own them and how many thousands of machines get routed through them... There is even a traceroute map somewhere that can give you an idea of how deeply dependant we are on these routers. It's been a long time since I stopped believing in security, the core of the security problem is really because we are trusting trust (read Ken Thomson's article, reflections on trusting trust), if I did believe in security then I wouldn't be selling penetration tests.

How many times have you heard people saying, "Hey I Own this cisco, it would be cool if I had IOS src... I could trojan and recompile it and do this and that.", how many times have you heard of people wondering what the [redacted] they could do with an enable password. The IOS src has been floating around for quite a while now and no-one's done anything with it yet; at least not among the regular bugtraq letspretendtofulldisclosure readers.

Well you don't even really need the IOS src, everything you need is already there, (there is only one little thing that would be nice to have from the src but we'll talk about it below). You can load up the image in IDA, nop out a couple of instructions and the cisco's rmon implementation won't zero the payload anymore and you have a IOS sniffer.

"Gaius", Phrack Magazine, Volume 0xa Issue 0x38, May 01, 2000

==== PHENOELIT ====



A remote Cisco IOS exploit

[Download](#) | [Tutorial](#) | [DEF CON X Slides](#) | [Black Hat Slides](#) | [License](#)

+++UPDATE+++

In contrast to what was said before on this topic, there are stack based overflows in Cisco IOS. One of them is the HTTP stack vulnerability ([Cisco security notice here](#)), which can be exploited stable using the UDP echo memory leak described [here](#). Grab the stuff from the [download section](#).

Rant

"FX" from Phenoelit, circa 2002

So why is this happening ?

Let's look at the threat landscape

The Evolving Threat Landscape

Perimeter

Pervasive

Attacks focused on:

Operating Systems

- Microsoft OS
- Linux
- Solaris

Attacks focus on:

Applications

- Databases
- Application suites
- 3rd-Party applications
- Web applications

Attacks will focus on:

Next Generation Technologies

- Collaboration suites
- Virtualization technology
- Networks
- SaaS & ITaaS

Yesterday

Minutes

Today

Seconds

Tomorrow

Instant

Attackers were:

Minimally Experienced

- Mischievous
- After notoriety
- Using virus payloads via e-mail

Attackers are:

Well Trained

- Trained hackers
- Professional gain
- Delivering malware via Web sites

Attackers will be:

Seasoned

- Attacks against primo suppliers
- Attack multiple computers and networks simultaneously
- Polymorphic

Hobbyists

Professionals

1997 – In the beginning . . .

```
From: jbash@cisco.com Sun Feb 15 05:18:16 1998  
Date: Mon, 10 Nov 1997 16:39:36 -0800  
From: John Bashinski  
To: BUGTRAQ@NETSPACE.ORG  
Subject: Cisco IOS password encryption facts
```

-----BEGIN PGP SIGNED MESSAGE-----

A non-Cisco source has recently released a new program to decrypt user passwords (and other passwords) in Cisco configuration files. The program will not decrypt passwords set with the "enable secret" command.

The unexpected concern that this program has caused among Cisco customers has led us to suspect that many customers are relying on Cisco password encryption for more security than it was designed to provide. This document explains the security model behind Cisco password encryption, and the security limitations of that encryption.

<http://insecure.org/splloits/cisco.passwords.html>

Look at the date - it's 1997. And someone thinks "Hmm... I wonder if those Cisco passwords can be reversed ?"

The screenshot shows the Cisco website interface. At the top, there is a navigation bar with links for 'Solutions', 'Products & Services', 'Ordering', 'Support', 'Training & Events', 'Partner Central', and 'My Cisco'. Below this is a search bar and a 'Go' button. The main content area is titled 'Cisco IOS Password Encryption Facts' with a document ID of 107614. A 'Downloads' section contains a link to 'Cisco IOS Password Encryption Facts'. A 'Contents' section lists various sub-topics such as 'Introduction', 'Prerequisites', 'Requirements', 'Components Used', 'Conventions', 'User Passwords', 'enable secret and enable password', 'Which Cisco IOS Image Supports enable secret?', 'Other Passwords', 'Configuration Files', 'Can The Algorithm Be Changed?', and 'Related Information'. The 'Introduction' section begins with the text: 'A non-Cisco source has released a program to decrypt user passwords (and other passwords) in Cisco configuration files. The program will not decrypt passwords set with the enable secret command. The unexpected concern that this program has caused among Cisco customers has led us to suspect that many customers are relying on Cisco password encryption for more security than it was designed to provide. This document explains the security model behind Cisco password encryption, and the security limitations of that encryption.'

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml

Next Step: DoS attacks

The screenshot shows the Cisco Security Advisory page for "Cisco Security Advisory: TCP Loopback DoS Attack (land.c) and Cisco Devices". The page includes a navigation menu with options like Solutions, Products & Services, Ordering, Support, Training & Events, Partner Central, and My Cisco. The main content area displays the document ID (13661), advisory ID (cisco-sa-19971121-land), and a URL. A red oval highlights the text "For Public Release 1997 November 21 2200 UTC (GMT)". A "Downloads" section on the right provides links to the advisory and Cisco Devices.

Worldwide [change] | Log In | Register | About Cisco

Search Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central | My Cisco

HOME | PRODUCTS & SERVICES | SECURITY ADVISORIES

Cisco Security Advisory: TCP Loopback DoS Attack (land.c) and Cisco Devices

Products & Services

Cisco Security Advisory: TCP Loopback DoS Attack (land.c) and Cisco Devices

Document ID: 13661

Advisory ID: cisco-sa-19971121-land

<http://www.cisco.com/warp/public/707/cisco-sa-19971121-land.shtml>

Revision 6.0

Last Updated 1997 December 11 0100 UTC (GMT)

For Public Release 1997 November 21 2200 UTC (GMT)

Downloads

- [Cisco Security Advisory: TCP Loopback DoS Attack \(land.c\) and Cisco Devices](#)

From wikipedia:

“The attack involves sending a spoofed **TCP SYN** packet (connection initiation) with the target host's **IP address** and an open port as both source and destination.

The reason a LAND attack works is because it causes the machine to reply to itself continuously.

Not specifically targeted at Cisco devices – but nonetheless, some devices were affected by this attack

Well, that didn't take long . . .

The screenshot shows the Cisco website's security advisory page. The main heading is "Cisco Security Advisory: 7xx Router Password Buffer Overflow". Below the heading, the document ID is 13666, and the advisory ID is cisco-sa-19971216-pw-buffer. A URL is provided: <http://www.cisco.com/warp/public/707/cisco-sa-19971216-pw-buffer.shtml>. The revision is 2.0, and it was last updated on June 16, 1998. A red oval highlights the text "For Public Release 1997 December 16 0100 UTC (GMT)".

Summary

Some Cisco 7xx routers can be crashed by connecting with TELNET and typing very long password strings. There exists a small possibility that this bug could be exploited to launch other attacks against the router, other than simply crashing it.

Exploitation and Public Announcements

Cisco has had no known reports of malicious exploitation of this vulnerability.

This vulnerability has been discussed on the "bugtraq@netSPACE.org" mailing list, and is therefore certain to be widely known in the cracker community. The first public announcement of this vulnerability of which Cisco is aware was on December 11, 1997.

The vulnerability can be exploited to crash systems with no special tools or knowledge; no exploitation program as such is required.

Skip a couple years

The screenshot shows the Cisco Security Advisory page for 'Cisco Security Advisory: IOS HTTP Authorization Vulnerability'. The page includes a navigation menu with 'Solutions', 'Products & Services', 'Ordering', 'Support', 'Training & Events', 'Partner Central', and 'My Cisco'. The main content area displays the following information:

- Document ID: 13626
- Advisory ID: cisco-sa-20010627-ios-http-level
- URL: <http://www.cisco.com/warp/public/707/cisco-sa-20010627-ios-http-level.shtml>
- Revision 1.8
- Last Updated 2003 September 23 0800 UTC (GMT)
- For Public Release 2001 June 27 1500 UTC (GMT)** (circled in red)

On the right side, there is a 'Downloads' section with a link to 'Cisco Security Advisory: IOS HTTP Authorization Vulnerability'.

Summary

When the HTTP server is enabled and local authorization is used, it is possible, under some circumstances, to bypass the authentication and execute any command on the device. In that case, the user will be able to exercise complete control over the device. All commands will be executed with the highest privilege (level 15).

Exploitation and Public Announcements

This vulnerability has been reported to us independently by David Hyams, Ernst & Young, Switzerland and by Bashis (bash@ns.wcd.se).

The Cisco PSIRT have learned that an automated exploit has been created. The scanning for and attempts of exploiting this vulnerability are increasing. All customers are strongly recommended to apply workarounds or to upgrade to the IOS version that is not affected.

And then someone releases a tool

The screenshot shows a Cisco website page for a security notice. The header includes the Cisco logo and navigation links like 'Solutions', 'Products & Services', etc. The main content area is titled 'Cisco Security Notice: Exploit for Multiple Cisco Vulnerabilities' and provides details such as 'Document ID: 50220', 'Revision 1.3', and 'Last Updated 2004 May 07 at 17:30 UTC (GMT)'. A 'Downloads' section on the right contains a link to the exploit tool.

Summary

Proof-of-concept code has been publicly released by an external group that exploits multiple previous vulnerabilities in various Cisco products.

Details

Proof-of-concept code has been publicly released by an external group that exploits multiple previous vulnerabilities in various Cisco products.

Cisco 677/678 Telnet Buffer Overflow Vulnerability
Cisco IOS Router Denial of Service Vulnerability
Cisco IOS HTTP Auth Vulnerability

...

Cisco IOS Software HTTP Request Denial of Service Vulnerability
Cisco 514 UDP Flood Denial of Service Vulnerability

...

Cisco IOS HTTP Denial of Service Vulnerability

The tool included “exploits” for a total of 14 previously disclosed vulnerabilities

It's 2004 – Recap of where we've come from

- 1997 – recover configuration passwords
- 1997 – first DoS attack targeting Cisco devices
- 1998 - 2000 – more DoS attacks
- 2001 – disclosure of file contents on CSS devices
- 2002 – authentication bypass, information disclosure on VPN3000 devices
- 2002 - 2004 – more DoS attacks

Continuing in 2004 ...

- We see a progression
 - Growing interest in network/embedded device security
 - Across customers, researchers, AND attackers
- The underground puts together a “Cisco attack toolkit” for known vulnerabilities
- And then someone wonders . . . **Is Cisco IOS vulnerable to the same kind of attacks as other operating systems?**

2005 – IOS Remote Code Execution

- Mike Lynn presents at BlackHat Las Vegas 2005 on remote IOS code execution
 - Previously believed to be “The Holy Grail”
- Mr. Lynn demonstrates an exploit for an IPv6 vulnerability.
 - Exploit is limited to local network, short lived, and allows for an attacker to connect to the device at privilege level 15.
 - No exploit code is released.
- Cisco publishes a Security Advisory and makes fixed software available to customers

Products & Services

Cisco Security Advisory: IPv6 Crafted Packet Vulnerability


Document ID: 65783

Revision 1.8

[Last Updated](#) 2005 August 11 1800 UTC

For Public Release 2005 July 29 0800 UTC

Downloads

[Cisco Security Advisory: IPv6 Crafted Packet Vulnerability](#) 

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>

And there is follow-up research on the subject

im InformationRiskManagement | Research Lab

Research Lab	Whitepapers
Whitepapers	
Bespoke and Collaborative Research	
Tools	
Advisories	
Disclosure Policy	
Conferences and Seminars	
Back	

- [Targeting VOIP](#)
Author Kendric Tang - Posted October 2008
- [Risky Business - Hacking the Trading Floor](#)
Author Gyan Chawdhary - Posted September 2008
- [IT Security and the Curse of Complacency](#)
Author Matthew Lewis - Posted January 2008
- [WebSphere MQ Threats: A Management Summary](#)
Author John Yeo - Posted November 2007
- [Creating Backdoors in Cisco IOS using TCL](#)
Author Andy Davis - Posted November 2007
- [High-Level Reverse Engineering](#)
Author Matthew Lewis - Posted October 2007
- [Biologger - A Biometric Keylogger](#)
Author Matthew Lewis - Posted September 2007
- [Security Testing Enterprise Messaging Systems](#)
Authors Andy Davis and Phil Higgins - Posted July 2007
- [IOS Exploitation Techniques](#)
Author Gyan Chawdhary - Posted June 2007
- [Everyday Password Cracking](#)
Author Thorsten Fischer - Posted June 2007

im InformationRiskManagement | Research Lab

Research Lab	Research Lab
Whitepapers	
Bespoke and Collaborative Research	Information technology constantly changes and advances. IRM is dedicated to keeping pace with new technology and continuing to innovate in the field of information security. This research website provides an opportunity for IRM's Research Working Group (RWG) to publish information on new and ongoing research programmes within IRM. Here you will find white papers, tools, security advisories and news on past and upcoming conferences and seminars at which IRM presents its research.
Tools	
Advisories	
Disclosure Policy	Latest news
Conferences and Seminars	Senior Consultants Gyan Chawdhary and Varun Uppal will be presenting their research on Cisco IOS Shellcode in Black Hat Las Vegas, August 6 2008.
Back	A copy of the presentation is available here (226k), with a video showing the bind shell here (6.6M WMV format).

The three shellcodes discussed in the presentation are available here:

- [Cisco IOS Tiny shellcode v1.0](#)
- [Cisco IOS Bind shellcode v1.0](#)
- [Cisco IOS Connectback shellcode v1.0](#)

The presentation covers significant advances in IOS shell code development and looks at its subsequent impact on modern day routing infrastructure. IOS specific payloads including bind shell, reverse shell, 2 byte shell codes and bypassing the check heaps process in IOS 12.4 are covered from both a practical and theoretical standpoint as well as a detailed overview of IRM's techniques used to develop these payloads. Furthermore, building a complete IOS debugging environment and identifying new attack vectors is also covered in the presentation, allowing researchers to establish a fully working environment to develop IOS specific code, execution payloads, memory resident backdoors and to conduct vulnerability research on Cisco embedded devices.

Importantly, the presentation also includes mitigating factors to the issues identified during this Cisco IOS research programme.

IRM Plc follows up on remote code execution research – publishing papers on 2007 and 2008

What Do Attackers See as the Next “Holy Grail?”

Rootkits

From wikipedia:

A **rootkit** is [malware](#) which consists of a [program](#) (or combination of several programs) designed to take fundamental control (in [Unix](#) terms "root" access, in [Windows](#) terms, "Administrator" access) of a computer system, without authorization by the system's owners and legitimate managers. Access to the hardware (e.g., the reset switch) is rarely required as a rootkit is intended to seize control of the operating system running on the hardware. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system [security](#) mechanisms. Often, they are [Trojans](#) as well, thus fooling users into believing they are safe to run on their systems. Techniques used to accomplish this can include concealing running processes from monitoring programs, or hiding files or system data from the [operating system](#).^[1]

NOTE: That definition doesn't translate 100% to Cisco IOS

And yes – someone created a rootkit for Cisco IOS

The screenshot shows the top of a web browser displaying the The Register website. The logo is prominent in red and white, with the tagline "Biting the hand that feeds IT". Navigation menus include categories like Hardware, Software, Music & Media, Networks, Security, Public Sector, Business, Science, Odds & Sods, and a search bar. Below the navigation, there are links for "Enterprise Security", "Anti-Virus", "Spam", "ID", and "Spyware". The main content area features a "Print story" button, a "Track this topic" button, and a "MOST READ" section with a list of articles. The article title is "Rootkits on routers threat to be demoed" by John Leyden, dated 15th May 2008. The article text mentions that security researchers have devised a rootkit for Cisco routers and that Sebastian Muniz of Core Security plans to demo it at the EuSecWest conference.

The Register
Biting the hand that feeds IT

Hardware Software Music & Media Networks **Security** Public Sector Business Science Odds & Sods Search site

Crime **Enterprise Security** Anti-Virus Spam ID Spyware Cash 'n' Carry Newsletters Feeds

Print story Track this topic

MOST READ MOST COMMENTED

- US kicks off secure hash competition
- Windows RPC exploit spawns bots and worms
- Microsoft rushes out emergency Windows update
- London consumers trounce corporates in wireless security
- Turbo-charged wireless hacks threaten networks

Rootkits on routers threat to be demoed
Networks own3d
By [John Leyden](#) • [Get more from this author](#)
Posted in [Enterprise Security](#), 15th May 2008 22:42 GMT

Updated Security researchers have devised a rootkit capable of covertly monitoring and controlling Cisco routers.

Sebastian Muniz, of Core Security, plans to demo Cisco IOS rootkit software he developed during a presentation at the [EuSecWest conference](#) in London on 22 May.

- Mr. Muniz' rootkit for Cisco IOS required:
 - Disassembly of a binary Cisco IOS image
 - Binary image patching
 - Loading of patched image on a Cisco IOS device, which requires privileged access to the device
 - Reloading of said device
- No code/tools were released. There is no “on-the-fly” injection.

And a Security Response was issued

The screenshot shows the Cisco Security Response Center interface. At the top left is the Cisco logo. To the right, there are links for 'Worldwide [change]', 'Log In', 'Register', and 'About Cisco'. Below this is a search bar with a 'Go' button. A navigation menu includes 'Solutions', 'Products & Services', 'Ordering', 'Support', 'Training & Events', 'Partner Central', and 'My Cisco'. The main content area is titled 'Products & Services' and 'Rootkits on Cisco IOS Devices'. It displays 'Document ID: 107193' and a link to the document: <http://www.cisco.com/warp/public/707/cisco-sr-20080516-rootkits.shtml>. Below the link, it shows 'Revision 2.1', 'Last Updated 2008 June 23 2300 UTC (GMT)', and 'For Public Release 2008 May 16 0400 UTC (GMT)'. On the right side, there is a 'Downloads' section with a link to 'Rootkits on Cisco IOS Devices' and a small icon of a document.

No new vulnerability on the Cisco IOS software was disclosed during the presentation. To the best of our knowledge, no exploit code has been made publicly available, and Cisco has not received any customer reports of exploitation.

It is possible that an attacker could insert malicious code into a Cisco IOS software image and load it onto a Cisco device that supports that image. This attack scenario could occur on any device that uses a form of software, given a proper set of circumstances. This Security Response will describe best practices that network administrators can use to reduce the risk that malicious code is installed on Cisco IOS devices. Additionally, this response will offer some methods that administrators can use to mitigate the risks of introducing malicious code into the network.

And we're going to talk more about this later 😊

2008 – the Present

- The threat landscape has evolved when it comes to embedded devices/network devices
- More researchers (both independent and within organizations) are taking a new look into exploiting network devices
- This is only normal and expected: after your “soft” targets (the end host) become “hard” targets, you start to look elsewhere
- The end host isn’t an island – it is connected to a network and exchanges data with other hosts, either on the same network or a different one
- If you lose control of the network, the host security becomes irrelevant
- **Whoever controls the network controls the information flowing through it**

The future (aka “let me check the crystal ball”) ☺



- **Additional research on remote code execution** – on Cisco devices running IOS, Cisco devices running other OSES and other vendors OSES
- **Research will combine attacks** – remote code execution paired with a trojan/rootkit payload, to hide compromise from the device administrator
- **Don't expect to see a “Cisco worm” loose** – whoever is able to develop working code might decide to sell it – and whoever buys it might keep it hidden until there is a need to use it
- **Portability of attacks** - Think about any attack against some other OS/platform, old or new, and assume the same attack will be replicated/ported to network devices (XSS, CSRF, etc. etc. etc.)

So what are we doing?

- Internal security testing of products, using both commercial and in-house tools
- Additional code reviews/hardening
- Developer education and training
- Enforcing of security best practices from product concept to shipping product
- Working closely with the research community and individual researchers
- Many other things . . .

Cisco Security Center: Mission Control

The screenshot displays the Cisco Security Center web interface. At the top, there is a navigation bar with links for 'Worldwide [change]', 'Log In', 'Register', and 'About Cisco'. A search bar is also present. Below the navigation bar, there are tabs for 'Solutions', 'Products & Services', 'Ordering', 'Support', 'Training & Events', and 'Partner Central'. The main content area is titled 'Security Center' and features a section for 'Inform, Protect, Respond' powered by 'IntelliShield'. A table of security alerts is shown, with columns for 'CVSS Score', 'Cisco IPS Signature', 'Cisco PSIRT Advisory', 'Cisco IntelliShield Mitigation Report', and 'Known Cisco Products Affected'. Several alerts are listed, including 'Microsoft Exchange IMAP Literal Processing Denial of Service Vulnerability' with a CVSS score of 9.3/2.4, 'Cisco IOS SSL ClientHello Message Denial of Service Vulnerability' with a CVSS score of 3.3/2.7 and a 'HOT' status, 'FS FirePass 4100 VPN my_activation.php3 Arbitrary Code Execution Vulnerability' with a CVSS score of 10.0/7.4, and 'Symantec Storage Foundation for Windows Scheduler Service Authentication Bypass' with a CVSS score of 2.3/0.7. A 'free trial' badge is visible near the bottom of the table. To the right of the table, there is an 'Important Message from John Stewart' section and a 'Cisco Emergency Response' section with contact information. Below the table, there are sections for 'Track and Analyze' (Threat Analysis and Reporting) featuring a world map with threat activity markers, and 'Improve Your Security' (Best Practice Guidance) with various resource links like 'Security Programs', 'Business Resources', 'Regulatory Compliance', 'Design Zone for Security', and 'Technical Resources'. A 'Security Top of Mind' section at the bottom right features an interview with John N. Stewart.

- CVSS Scores
- IPS Signatures
- PSIRT Security Alerts
- Applied Mitigation Bulletins
- Integration with IronPort
- Six month free trial
- Single point of access
- Dynamic content

And what should YOU be doing ?

- **Keep devices updated with security fixes** – if you're still running 10+ years old software, chances are you're vulnerable to multiple issues
- **Subscribe to vendors security announcement list** – and read those announcements, analyze if and how they apply to your environment, and act upon said analysis.
- **Implement security best practices**, including but not limited to: AAA, logging, event analysis and correlation
- **Limit access to network devices** – and monitor all access to said devices.
- **Implement an incident response plan** – and schedule training exercises to make sure it will work when needed

Some closing thoughts

- Do not get overwhelmed
- At the end of the day, this is a good thing – more research on network device security makes for better products
- Keep updated on security developments
- Be prepared
- If you see me running . . . 😊



Q and A



