Interested in learning more about security?

SANS Institute InfoSec Reading Room

Code Red Worm - Importance of Swiftly Eliminating Vulnerability

Hundreds of thousands of computers and network devices have been affected by three malicious programs unleashed through the Internet. Network latency and DoS attacks affected users throughout the world. System administrators, security professionals, and users spent an enormous amount of time in reaction to this threat. There remains an unknown number of servers operating with a wide-open back door, waiting for an intruder to stumble upon it. Lists of vulnerable servers are scattered throughout the globe in various logs...

GSEC Practical – v.1.2f (August 2001)

Code Red Worm – Importance of Swiftly Eliminating Vulnerability

Scotty Strunk

August 13, 2001

Over a seven-week period in the summer of 2001, a series of events unfolded that not only threatened over a quarter of a million computers but the infrastructure of the Internet itself. A vulnerability in Microsoft's IIS (Internet Information Server) software was announced, and a Webpage was created to provide the means to remove it. During this time, three different worms were released that exploited this vulnerability. A worm distinguishes itself from a virus in its ability to replicate and spread itself to other hosts using its own software code. This allows it to operate without relying on user interaction or having to attach itself to another program for transport. Code Red versions 1 & 2, and Code Red II infected IIS Web servers, causing exploited systems to search for and infect other vulnerable hosts via the Internet and some private networks. "The Chinese government says the Code Red II Internet worm has caused the most widespread computer disruption yet recorded on the country's networks, hitting more than 20 provinces and cities." [1] Vulnerable computers could have been patched or had an exploitable component disabled. Despite this, countless systems are missing the patch or are still infected. Even worse, Code Red II installs a Web-accessible back door with administrator privileges, leaving the victimized computer open to further, more heinous attacks. Experts still argue over who is to blame for these remaining infected and/or unpatched computers. Some blame the software manufacturer, while others blame the system administrators. Why weren't these systems patched and protected from this vulnerability?

On June 18, 2001, Microsoft published a Security Bulletin concerning an unchecked buffer in an Index Server ISAPI (Internet Server Application Programming Interface) extension. The specific .dll file extension vulnerable in IIS versions 4.0, 5.0 and 6.0 is idq.dll, which is used in the indexing service. It also supports administrative scripts (.ida files) and Internet Data Queries (.idq files). It is susceptible to a buffer overrun in the portion of the code that works with input URLs (Uniform Resource Locators). This particular buffer overrun vulnerability, also called the .ida vulnerability, exists on Microsoft Web servers running Windows NT 4.0, 2000 and XP beta 2, if IIS 4.0, 5.0 or 6.0 is installed. For Windows NT 4.0 and 2000 Professional OS's (Operating Systems), IIS must be explicitly installed. Windows 2000 and XP install IIS 5.0/6.0 by default, regardless of whether the user intends to utilize the computer as a Web server.

By crafting a certain URL, an attacker could easily execute arbitrary code on the system with local system administrator privileges. Bottom line, an intruder could "own" the Web server remotely through a HTTP (HyperText Transfer Protocol) session. A patch was made available to correct the code by adding proper input checking, eliminating the vulnerability, and instructions were also given to prevent the vulnerability from being exploited by removing certain script mappings. However, the addition or removal of certain components later could enable the vulnerability again.

Microsoft's bulletin credits eEye for the discovery. Riley Hassell found IIS's susceptibility to this buffer overflow attack while doing research on unknown vulnerability protection for one of eEye's products. Abruptly, one of his lab Web servers crashed. It was discovered that during the conversion of the one byte per character ASCII (American Standard Code for Information Interchange) input buffer filter into a two bytes per character (wide) Unicode string, no checking is performed on length. An attacker can use this vulnerability of the .ida ISAPI buffer to overwrite the EIP

[1] Tang, p.1

(Executive Interface Program) and run their own code at the local system privilege level. They developed working exploits for Windows NT 4.0 and 2000 and promised to post a proof-of-concept, illustrating file writing, to their Web site. Although eEye sent Microsoft an exploit code demonstrating shell binding (total control of target system), they stated that this code would not be released to the public.

At the time, the number of IIS Web servers was estimated at 5.9 million. This number did not include internal network systems, so the total number of vulnerable systems could have been much higher. Since actual risk also depends on factors, such as network configuration and environment, it is difficult to accurately access potential damage. After Microsoft announced the .ida vulnerability, system administrators, computer security professionals, and users began to patch their IIS servers or disable the vulnerability. This process of securing systems was sporadic, leaving many computers untouched, because of administrators who either didn't know about the security hole or didn't care. Also, this was the second advisory concerning a Microsoft buffer overflow vulnerability in less than two months. With the availability of high speed Internet access (DSL [Digital Subscriber Line] and cable modems), an increasing number of small businesses and end users connect servers to the Internet, having no knowledge of computer or network security. Over the next several weeks, online magazine articles and mailing lists discussed this vulnerability, and exploit code was published. It seemed that this would be yet another in a constant stream of published software vulnerabilities.

This security hole was about to become front-page news, as a serious threat was unleashed. Security experts began receiving and analyzing reports & logs of a suspicious activity. Evidence emerged that a worm program was using the buffer overflow vulnerability to infect IIS Web servers, and then causing the exploited servers to search for other vulnerable servers. eEye analysts received worm data on July 13th, and published their findings on the 17th. They named the worm Code Red, based on the Web defacement text "Hacked by Chinese", and a flavor of Mountain Dew that happened to be in the lab during a night of long hours of malware code disassembly. eEye provided an excerpt of packet data from the worm to help others configure IDS's (Intrusion Detection System) to detect Code Red. Some network administrators reported their logs, revealing approximately 5,000 unique IP addresses from hosts initiating attacks over three days. Disassembly of the Code Red worm showed an infected host will create multiple threads (100) in a loop to scan IP addresses, in search of servers. While the generation of these target IP addresses is random, the seed is the same in each worm. So, IP addresses attacked based on this "random" list will be attacked again as new hosts are infected. Once released, the worm checks the Microsoft OS and determines if English is the default language. If it is, the worm defaces pages with the text: "HELLO! Welcome to http://www.worm.com! Hacked By Chinese!"

On July 19th, Carnegie Mellon's CERT (Computer Emergency Response Team) published their "Code Red" Worm Advisory. It listed the same affected systems as those in Microsoft's bulletin, plus several Cisco systems, including the 600 series DSL routers. Initially, experts did not realize that the worm behavior was time sensitive, but further analysis showed other actions of the worm as dependent on the day of the month:

> "Day 1 - 19: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm.
>
> Day 20 - 27: A packet-flooding denial of service attack will be launched against a particular fixed IP address
>
> Day 28 - end of the month: The worm "sleeps"; no active connections or denial of service."[2]

The specific IP address the worm was programmed to attack is 198.137.240.91, which was the address associated with whitehouse.gov. Since the IP address was hardcoded in the worm, the associated address was simply changed to 198.137.240.92, effectively preventing further DDoS (Distributed Denial of Service). Normal browser traffic resumed to www.whitehouse.gov.

SARC (Symantec Anti-Virus Research Center) claimed a discovery date of July 16th, and listed the following aliases: W32/Bady, I-Worm.Bady, Code Red, CodeRed, and W32/Bady.worm, along with other information about the worm on their Web site. SARC and eEye provided access to free tools (Code Red Removal Tool and Code Red Scanner) to check vulnerability. The Code Red Scanner allowed users to check all IP's in a class C address range (254 addresses) for exploitability. McAfee's AVERT (Anti-Virus Emergency Response Team) also posted Code Red worm information and an assessment tool called CyberCop Worm Scan on their Web server. Also on July 19th, the SANS (System Administration Networking and Security) Institute published a security alert concerning the Code Red worm and, due to it's rapid spread, upgraded the Internet's INFOCON (Information Operations Condition) Alert Status to "Yellow" (Initial level of heightened alert), hosted at Incidents.Org. On July 22, SecurityFocus.com's Alfred Huger said that the ARIS (Attack Registry Intelligence Service) project had informed over 27,000 domains, containing over 172,000 IP's (unique) concerning possible worm infections.

A variant of the Code Red worm was discovered and dubbed CRv2. Unlike the original worm that uses a fixed seed to generate its victim IP address list, CRv2 uses a random seed. Over 350,000 hosts (unique) were detected as infected in a 24-hour period between July 19th and 20th. CAIDA (Cooperative Association for Internet Data Analysis) detected the first version of Code Red on July 12th, and CRv2 on July 17th. They examined infected host attributes (domains, geographic locations, top level domains) and listed the CRv2 location distribution:

> "Top 10 Countries

Country	#	%
US	157,694	43.91
KR	37,948	10.57
CN	18,141	5.05
TW	15,124	4.21
CA	12,469	3.47
UK	11,918	3.32
DE	11,762	3.28

[2] Danyliw, p.2

AU	8,587	2.39
JP	8,282	2.31
NL	7,771	2.16"[3]

The high percentage from the United States wasn't as much of a surprise as the ten percent figure from Korea.

As August 1st arrived, security experts and system administrators braced for the Code Red variants to resume their attempts to infect susceptible IIS servers and bombard the Internet with their traffic. There was also much discussion about the accuracy of the estimated numbers of infected servers. One of the theories was that intentional host probing was hiding amongst the Code Red scans. Sampling the approximately 360,000 infected systems detected in July, CAIDA estimated more than 30% of the computers are still at risk. On August 4th, HTTP probes increased unexpectedly, and packet analysis revealed the emergence of a new worm exploiting the same .ida IIS vulnerability. Examination showed it not to be a variant of the Code Red worm, but a new program.

It was named Code Red II. One of the characteristics that set this worm apart from the others is its malicious payload. It attacks a host (randomly chosen) on the normal HTTP service port of 80, and sends a special HTTP GET request. This crafted string exploits the IIS buffer overflow vulnerability, and the same process occurs with each of the other systems it attempts to self-replicate to. However, due to either a programming mistake or a warning by the worm author, the consequences of the attack vary according to the system and its configuration:

> "Unpatched Windows 2000 servers running IIS 4.0 or 5.0 with Indexing Service installed are likely to be compromised by the 'Code Red II' worm.
>
> Unpatched Windows NT servers running IIS 4.0 or 5.0 with Indexing Server 2.0 installed could experience crashes of the IIS server.
>
> Unpatched Cisco 600-series DSL routers will process the HTTP request thereby exploiting an unrelated vulnerability which causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
>
> Patched systems, or systems not running IIS with an HTTP server listening on TCP port 80 will probably accept the HTTP request, return with an 'HTTP 4xx' error message, and potentially log this request in an access log."[4]

If the worm succeeds in infecting the host, it performs several tasks. One of which is checking the victim host for an identifier from a previous infection. If found, it deactivates itself. If not, it continues the infection. The default OS language is checked, and based on the outcome, the worm creates the number of threads used for propagation. If the language is Chinese, Code Red II causes a 48-hour scan using 600 threads, or if not, a 24-hour scan with 300 threads. Then the worm copies a shell

[3] Moore, p.5
[4] Danyliw, p.2

program, CMD.EXE, into several public directories on the server. This provides an opportunity to run arbitrary code with the same privileges as the process (IIS server). Next, a fake EXPLORER.EXE (Trojan horse) is copied to the root of logical drives C and D, and these directory paths are opened up by virtual mapping. The Trojan hides its existence by calling the real executable, and runs every time a user logs on (on computers vulnerable to the "Relative Shell Path" exploit[5]). The existence of "C:\explorer.exe" or "D:\explorer.exe" can indicate infection, as well as "root.exe" in the IIS scripts and MSADC (Microsoft Active Directory Connector) folders. The presence of "root.exe" is not conclusive, because there is another worm, "sadmin Unicode," that also renames "cmd.exe" to "root.exe."

SARC encountered Code Red II on August 4th, and provided the following AKA's (Also Known As): CodeRed.v3, CodeRed.C, CodeRed III, and W32.Bady.C. They considered it a variant of the first Code Red worm because of the common exploit used to gain control over the victim host. They, along with others, referenced the original Microsoft Security Patch for IIS buffer overflow vulnerability and listed steps to remove traces of the infection. Once compromised, a computer needs to be thoroughly examined for other Trojans and back doors that an intruder may have left. A good general reference for compromised systems is CERT's "Steps for Recovering from a UNIX or NT System Compromise"[6]. The greatest damage that Code Red II does is the installation of a "back door" on an exploited server, available to anyone via a simple HTTP port 80 connection. The automated replication properties of the worm will cause DoS (Denial of Service) for portions of the Internet, servers near worm infections, and some Cisco routers and devices.

27 days passed between Microsoft's announcement of an Index Server ISAPI extension buffer overflow vulnerability, and NIPC's (National Infrastructure Protection Center [United States]) "Reduction of Code Red Threat" statement in their Assessment 01-018. Hundreds of thousands of computers and network devices have been affected by three malicious programs unleashed through the Internet. Network latency and DoS attacks affected users throughout the world. System administrators, security professionals, and users spent an enormous amount of time in reaction to this threat. There remains an unknown number of servers operating with a wide-open back door, waiting for an intruder to stumble upon it. Lists of vulnerable servers are scattered throughout the globe in various logs and scan lists, offering tempting information to Black Hats, crackers and script kiddies. All of this because a patch was not applied. Patching a vulnerable system takes only a few minutes and a reboot, so why were these system not patched? The answer has many parts: the OS should not have been vulnerable in the first place; many users never realized they were vulnerable; the shear volume of vulnerabilities & security bulletins every month; lack of education of users; and understaffed & overworked system administrators. This is no excuse. We as security professionals have an obligation to mitigate the risk of having a world with interconnected computers.

[5] Microsoft
[6] Carnegie

References:

Carnegie Mellon University. “Steps for Recovering from a UNIX or NT System Compromise.” CERT® Coordination Center. 17 Apr. 2000. URL: http://www.cert.org/tech_tips/win-UNIX-system_compromise.html (13 Aug. 2001).

Cisco Systems. “Cisco Security Advisory: ‘Code Red’ Worm - Customer Impact.” Revision 2.2. 11 Aug. 2001. URL: http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml (15 Aug. 2001).

Danyliw, Roman and Householder, Allen. “CERT® Advisory CA-2001-19 ‘Code Red’ Worm Exploiting Buffer Overflow In IIS Indexing Service DLL.” 30 Jul. 2001. URL: http://www.cert.org/advisories/CA-2001-19.html (13 Aug. 2001).[2]

Danyliw, Roman; Householder, Allen and Lindner, Marty. “CERT® Incident Note IN-2001-09 ‘Code Red II:’ Another Worm Exploiting Buffer Overflow In IIS Indexing Service DLL.” 6 Aug. 2001. URL: http://www.cert.org/incident_notes/IN-2001-09.html (13 Aug. 2001).[4]

eEye Digital Security. “.ida ‘Code Red’ Worm” Research, Advisory AD20010717. 17 Jul. 2001. URL: http://www.eeye.com/html/Research/Advisories/AL20010717.html (13 Aug. 2001).

eEye Digital Security. “All versions of Microsoft Internet Information Services Remote buffer overflow (SYSTEM Level Access).” Research, Advisory AD20010618. 18 Jun. 2001. URL: http://www.eeye.com/html/Research/Advisories/AD20010618.html (13 Aug. 2001).

Meeks, Brock N. “Microsoft Web security hole found.” MSNBC News. 18 Jun. 2001. URL: http://www.msnbc.com/news/588963.asp#BODY (13 Aug. 2001).

Microsoft. “Microsoft Security Bulletin (MS00-052).” Microsoft TechNet. 28 Jul. 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-052.asp (13 Aug. 2001).[5]

Microsoft. “Microsoft Security Bulletin MS01-033.” Microsoft TechNet. 18 Jun. 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp (13 Aug. 2001).

Moore, David. "The Spread of the Code-Red Worm (CRv2)." 1 Aug. 2001. URL: http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml (15 Aug. 2001)

NIPC. "Code Red Reminder and Clarification." ASSESSMENT 01-018. 16 Aug.2001. URL:
http://www.nipc.gov/warnings/assessments/2001/01-018.htm (22 Aug. 2001

SANS Institute, The. “Handler's Diary - August 2001.” 15 Aug. 2001. URL:
http://www.incidents.org/diary/august2001.php

SANS Institute, The. “INFOCON DESCRIPTIONS.” 15 Aug. 2001. URL:
http://www.incidents.org/infocon.php

Tang, Rose. “China's networks hit by Code Red II.” CNN.com./WORLD. 10 Aug. 2001. URL:
http://www.cnn.com/2001/WORLD/asiapcf/east/08/10/china.codered/index.html (13 Aug. 2001).

Last Updated: December 17th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	OnlineCAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced