Global Information Assurance Certification Paper

The Mechanisms and Effects of the Code Red Worm
GSEC Practical Assignment Version 1.2f
Renee C. Schauer

Introduction

It is common for viruses, hacker attacks and system vulnerabilities to make the evening news on an almost weekly basis. Web sites such as SANS and CERT are updated daily with new viruses, worms and security holes. It has become a difficult task for system administrators to keep up with the task of securing their systems. Not only must they know about the constantly changing vulnerabilities that are present in software and hardware, but they must also continue to monitor for attacks, patch for new viruses and control access of internal users.

Exploits can come in many forms. Viruses such as "I Love You" and "Melissa" can affect individual computers and web traffic through launching email attachments with malicious code. Denial of Service attacks send traffic to flood servers and bring them down. But a worm is an exploit that is often times more effective than other methods because it invades servers overwhelming the memory capacity and then shuts down before the worm is passed automatically to another machine. It is also effective because it does not rely on infected files spreading through the "cooperation" of a user opening an email attachment or launching a program.

Recently an exploit was identified and named Code Red. This worm caused billions of dollars in damages and introduced to the technology community the dangers of not reacting quickly to public warnings of vulnerabilities. This paper addresses the vulnerability that was present in Microsoft Internet Information Services (IIS) web server software and the worm, Code Red, which exploited this vulnerability. It describes the mechanisms of three different versions of Code Red, as well as the patches and methods for stopping the worm. Finally, it discusses the effects of the worm, both financially and technically, as well as in how it has impacted the security of systems in general.

Discovery of the Vulnerability

The beginning of the Code Red crisis began with the discovery of a vulnerability. Riley Hassell, an employee at eEye Digital Security was running CHAM auditing code against eEye's Microsoft IIS web server to check for unknown software vulnerabilities. He identified that there was a buffer overflow vulnerability due to a section of code that performs input parameters which contained an unchecked buffer in the ISAPI extension. Hassell realized that this could enable an attacker to perform a buffer overrun attack and take complete control of the server and run foreign code.

On June 18, 2001, eEye Digital Security released an advisory notifying users that a remote buffer overflow vulnerability existed in Microsoft IIS web server software. The advisory indicated that Microsoft web servers Windows NT 4.0 IIS 4.0, Microsoft Windows 2000 IIS 5.0 and Microsoft Windows XP beta IIS 6.0 were all susceptible to the Index Server ISAPI vulnerability which could be used to take control of a server by specially formatting a web page request. According to the CAIDA Analysis of Code Red, the vulnerability resides in the code that allows a web server to interact with the Microsoft Indexing Service functionality. With a default installation of the Indexing Service ISAPI filter, the .ida ISAPI filter performs improper bounds checking of user inputs. This makes the filter predisposed to buffer overflow attacks.

If an attacker is aware of the vulnerability, they can gain full system level access remotely to the web server. This full system access allows the outsider to perform any action including executing programs, manipulating web server databases and changing files and web pages. In the eEye advisory the following comment was made, "Some people might wonder why this advisory does not contain the typical eEye humor like most of our other advisories. Basically, the reason is that this is our 4th remote system level IIS vulnerability and well…we've run out of jokes." They advised users to download a patch made available for the vulnerability from Microsoft and to remove the .ida ISAPI filter from the web server if it did not provide the server with any needed functionality.

A Long Night

The Code Red worm version 1 began to infect Microsoft IIS web servers on July 12, 2001. The next evening, two employees of eEye Digital Security pulled an "all-nighter" to disassemble and analyze the worm fueling their efforts with the heavily caffeinated "Code Red" Mountain Dew. Their beverage of choice along with the fact that the worm defaces many web pages with "Hacked by Chinese" led to the name Code Red.

It was determined that the virus spread through port 80 TCP/IP transmissions. A TCP/IP stream was sent to vulnerable web servers, and then a scan was performed to identify additional systems that were vulnerable. There were several versions and variants of Code Red that would surface in the next couple of weeks. The following sections describe the inner workings and effects of each virus.

Code Red Version 1

Servers that had not patched the Index Server ISAPI buffer overflow vulnerability were first infected with Code Red version 1 on July 12, 2001. The Code Red worm version 1 first checked the server date to see if the date was between the first and the nineteenth of the month. If it met this criterion, a static seed was used to generate a list of random IP addresses to probe each machine to attempt to infect as many computers

as possible. The use of the static seed in the random number generator resulted in the same list of IP addresses being generated for each infected machine. The worm spread slowly as each infected machine spread the worm to other machines.

On the twentieth of the month, Code Red version 1 was programmed to cease attempts to spread the virus to other machines. Instead, the worm was supposed to launch a Denial of Service attack against the White House web site (www1.whitehouse.gov) between the 20-28th of the month and then hibernate before beginning the cycle on the first day of the next month. The White House web site avoided the Denial of Service attack by changing its IP address when the threat was identified. However, a design flaw was noted in the Code Red source code. The code checked for a valid connection before sending data to perform the Denial of Service attack, and since the IP address was no longer valid, the connection was never established. Therefore, traffic did not increase as a result of trying to access the Whitehouse.gov web site.

Although Code Red version 1 defaced some web pages with "Hacked by Chinese" and consumed some resources on local area networks and infected web servers, it did not cause much damage and had little impact on global resources. This is partially due to the fact that the infected systems ended up reinfecting each other since a static seed created the IP address list.

The Code Red version 1 was memory resident meaning that the machine can be disinfected by rebooting it since it did not write to the system's hard disk. Rebooting, however, still left the system open to repeat infection, and with version 1 reinfection was an extreme possibility due to the list of IP addresses occurring in the same order due to the static seed.

Code Red Version 2

The second version of Code Red was discovered at 10:00am on July 19th. This version of the worm varied in that the random number generator used a random seed variant as opposed to the previous static seed. This caused each infected computer to infect a different list of randomly generated IP addresses. While this change seems minor, the effect was that more than 359,000 machines were infected in fourteen hours by Code Red version 2. At the peak of infection, 2000 hosts were infected each minute.

This version of the worm also affected additional devices such as DSL modems, printers, switches and routers. HP web servers and other hardware equipped with interfaces to the web could crash if scanned by Code Red. Cisco's web site confirmed that products including DSL routers, IP phones and wireless networking access kits were vulnerable to Denial of Service due to the Code Red virus. These devices were not infected with Code Red, but would crash or reboot when they were sent a copy of the worm by an infected machine.

Although Code Red version 2 was similar in its inner workings to version 1, it caused much more damage due to the volume of machines infected and probes sent to infect new hosts. The effects on additional hardware also increased the downtime and effects of the worm.

Similar to Code Red version 1, version 2 could be removed from the machine by rebooting. However, reinfection was occurring so quickly that many machines were reinfected as the patch for the .ida vulnerability was applied.

Code Red II

On August 4, 2001 the Code Red II worm began to exploit the Microsoft IIS web server buffer overflow vulnerability. This virus, while completely different than the original Code Red, was named after Code Red because the source code contained the string "CodeRedII." Unlike the original Code Reds, this worm did not deface the web page or launch Denial of Service attacks. However, the mechanism of this exploit was much more concerning and consequential than the original two.

The attack mechanism began with the worm checking a new host to the to see if the system had been previously infected. It also looked to check whether Chinese was the language of the system. If so, it spread for 48 hours using 600 threads. If the system was not set with Chinese as the language, it created 300 threads and spread for 24 hours. The virus then rebooted the system and cleared the worm portion from memory. However, most systems were immediately reinfected or the reboot would occur over and over. The rebooting action was the action that caused the worm to spread to the next infected machine identified.

The worm was also created with a mechanism to load a Trojan and toggle file system protection to publish C: and D: drives as web pages. The Trojan was saved to c:\explorer.exe and d:\explorer.exe and was run when Explorer.exe was called. The Trojan wrote values to the registry to open a security hole in the system to allow a remote attacker access via a web browser to the C: and D: drives. The backdoor installed could be used to launch future attacks or to execute any code.

The Code Red II virus is not memory resident, and therefore cannot be removed by rebooting the machine. In order to fix a system infected with Code Red II, the system had to be patched to prevent reinfection and then the worm removed.

Preventing the Virus from Infecting

The only way to prevent an infection of a Microsoft IIS web server was to patch the system with a download available from Microsoft at the following URL:

http://www.microsoft.com/technet/treeview/devault.asp?url=/technet/itsolutions/security/topics/codealrt.asp

Representatives from Microsoft and United States security agencies held a press conference instructing users to download the patch available from Microsoft and indicated it as “a civic duty” to download this patch. CNN and other news outlets following the spread of Code Red urged users to patch their systems. As of August 1, one million users had downloaded the patch that would prevent infection by all versions of the Code Red worm. The effects of the exploit were reduced by the publicity the worm received. However, the patch had been announced five weeks prior to Code Red’s emergence, and many security administrators waited until a threat was imminent to patch these systems. Some administrators even delayed patching their systems when Code Red version 1 became quiet and did not attempt to apply patches until version 2 began spreading ten days later.

Symantec Security Response recommended downloading the Microsoft patches as opposed to trying to detect the infection by searching for specific files written by the worm or defaced web pages. Since the virus runs only in memory and does not write information to the hard drive the virus could not be reliably detected. Applying the patch from Microsoft and restarting the computer was the only foolproof way to remove Code Red and prevent reinfection.

Some programs have also been developed to help eliminate the Code Red worm. CodeGreen is a program that waits for the worm to infect a system, and then launches a counter-attack to remove the worm and install a patch automatically. Crclean is another program used to destroy Code Red when it attempts to infect a system.

Effects of the Virus

The main effects of the Code Red viruses were performance degradation and system instability. The worldwide cost of the Code Red was $2.6 billion in July and August, which included cleaning and inspecting servers for $1.1 billion dollars and productivity losses of $1.5 billion dollars. The Code Red worm’s costs were widespread and devastating to many companies. It was estimated that over one million of the 5.9 million Microsoft IIS web servers were infected by Code Red. Many companies experienced internal disasters when 25 or more system infections simultaneously occurred or large segments of the network were disabled when hardware devices were scanned. The average outage for these large companies was 36 hours.

The cost of computer viruses in general has risen drastically over the past two years. According to the Computer Economics of Carlsbad, CA the cost of virus attacks on information systems in 2001 reached $10.7 billion so far this year as compared to $17.1 billion for 2000 and $12.1 billion in 1999.

Who Did This?

There is no clear evidence as to where the Code Red worm originated, however there are some theories. Keith Rhodes, the chief technologist for the General Accounting Office released in a congressional report that the Code Red virus is believed to have started at Foshan University in Guangdong, China. Some feel China is a prime suspect due to the worm being launched shortly after the mid-air collision of an American military spy plane and a Chinese fighter jet. School officials had reported a dramatic increase in web traffic around the time of Code Red's origination. However, university computer department personnel indicated that the school was on vacation at the time and the lab was being refurbished. Other intrusion detection logs compiled by Dshield.org indicated that the virus hit the United States and other countries before moving to Foshan University. Ken Eichman, senior security engineer for CAS, stressed that the hacker could have infected the server from a remote location so it is difficult to say it came from the university.

Others blamed the Chinese due to the messages "Hacked by Chinese. Welcome to http://www.worm.com." Johannes Ullrich, operator of the Dshield.org service indicated that "tracking down 'patient zero' or the first machine infected with Code Red I is difficult, because the worm does not leave any files behind on infected systems." He also theorized that an attendee of DefCon, the annual hacker convention held in Las Vegas on July 13, could have launched the virus. At a recent hacker convention in the Netherlands, it was speculated that the creator could have been present at the activities. Participants were heard to say that they hoped police got to the hacker before system administrators did!

Lessons Learned from Code Red

According to surveys conducted since Code Red's emergence, the publicity and effects of this and other recent large viruses have caused an increase in management-level attention to security issues. A Global Information Security Survey conducted by PricewaterhouseCoopers indicated that 41% of CEOs, company presidents and managing directors are now involved in creating security policy and 52% of top executives are involved in security budgeting decisions. These figures show more than a 10% increase from the previous year.

Unfortunately, even increased monitoring and increased awareness about exploits does not solve the problems of keeping up with security vulnerabilities. System administrators are required to monitor security sites, vendor sites and intrusion detection logs on a daily basis to keep up with constantly changing security issues. If the current trend of three new security vulnerabilities announced everyday continues, it will become even more difficult, if not impossible, for security managers to manage the problem.

The good news about the Code Red worm is the publicity it gave to securing web servers. David Moore, a senior researcher with CAIDA indicated, “Code Red got a lot of publicity. It got a lot of people recognizing that patching servers is a problem.” A Netcraft survey indicated that many security administrators started patching servers for the first time when Code Red became an issue. By scanning a few hundred systems each month for ten security lapses, Netcraft found that eight of the vulnerabilities decreased drastically by the end of August as security administrators started to take web server patching more seriously. Hopefully, the Code Red outcomes will be a warning to companies to dedicate adequate resources to security administration and increase awareness of the need to patch security holes and continue monitoring for the next exploit.

References:

"All Versions of Microsoft IIS Remote Buffer Overflow." June 18, 2001. http://www.eeye.com/html/Research/Advisories/AD20010618.html

Chien, Eric. "CodeRed Worm." Symantec Security Response. August 27, 2001. http://www.symantec.com/avcenter/venc/data/codered.worm.html

"Code Red Virus Likely Originated in China." Business Recorder. September 2, 2001.

Fruitman, Paul. "Code Red Worm Sluggish to Hit." Computing Canada: ProQuest Information and Learning, August 10, 2001.

Hulme, George. "Management Takes Notice – High-Profile Web Attacks and Viruses are Convincing Upper Management At Many Companies to Take Security Seriously." Information Week. CMP Media LLA. September 3, 2001, p. 28.

Lemos, Robert. "Internet Security Helped by Code Red." Special to CNET News.com. September 7, 2001.

Lemos, Rob. "Virulent Worm Calls Into Doubt Our Ability to Protect the Net." Special to CNET News.com. July 27, 2001.

Lemos, Rob. "Web Worm Targets White House." Special to CNET News.com. July 19, 2001.

Leyden, John. "Code Red's Cisco Side Effect." August 13, 2001. http://www.secuityfocus.com/templates/article.html?id=235

McWilliams, Brian. "Code Red: Born In the USA?" Newsbytes. August 31, 2001. http://www.nbnn.com/news/01/169636.html

Saita, Anne. "Code Red's Costs and Hunt for Creator Mount." Information Security Magazine. Security Wire Digest, Vol. 3, No. 68. September 6, 2001. http://www.infosecuritymag.com/current_daily.html

"Technology Netviews – Systems Are Crumbling Under Weight of Apathy." Network News, VNU Business Publications Ltd., September 5, 2001, p. 26.

"W32/CodeRed.a.worm." McAfee – AVERT. July 30, 2001. http://vil.nai.com/vil/virusChar.asp?virus_k=99142

Wilson, Pat and Brian Kantor. "CAIDA Analysis of Code-Red." August 25, 2001. http://www.caida.org/analysis/security/code-red/