CERT Advisory CA-2001-23 Continued Threat of the "Code Red" Worm

Original release date: July 26, 2001
Last revised: January 17, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
- Unpatched Cisco 600 series DSL routers

Overview

Since around July 13, 2001, at least two variants of the self-propagating malicious code "Code Red" have been attacking hosts on the Internet (see CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL). Different organizations who have analyzed "Code Red" have reached different conclusions about the behavior of infected machines when their system clocks roll over to the next month. Reports indicate that there are a number of systems with their clocks incorrectly set, so we believe the worm will begin propagating again on August 1, 2001 0:00 GMT. There is evidence that tens of thousands of systems are already infected or vulnerable to re-infection at that time. Because the worm propagates very quickly, it is likely that nearly all vulnerable systems will be compromised by August 2, 2001.

The CERT/CC has received reports indicating that at least 280,000 hosts were compromised in the first wave.

A translation of this advisory into Polish is available at http://www.cert.pl/CA/CA-2001-23-PL.html.

I. Description

The "Code Red" worm is malicious self-propagating code that exploits Microsoft Internet Information Server (IIS)-enabled systems susceptible to the vulnerability described in CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. Its activity on a compromised machine is time senstive; different activity occurs based on the date (day of the month) of the system clock. The CERT/CC is aware of at least two major variants of the worm, each of which exhibits the following pattern of behavior:

- **Propagation mode (from the 1st - 19th of the month)**: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm. Depending on the configuration of the host that receives this request, there are varied consequences.
  - *Unpatched IIS 4.0 and 5.0 servers with Indexing service installed* will almost certainly be compromised by the "Code Red" worm. In the earlier variant of the worm, victim hosts with a default language of English experienced a defacement on all pages requested from the web server. Hosts infected with the later variant did not experience any change in the served content.
  - *Unpatched Cisco 600-series DSL routers* will process the HTTP request and trigger an unrelated vulnerability that causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
  - *Systems not running IIS, but with an HTTP server listening on TCP port 80* will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log.
- **Flood mode (from the 20th - 27th of the month)**: A packet-flooding denial-of-service attack will be launched against a specific IP address embedded in the code.
- **Termination (after the 27th day)**: The worm remains in memory but is otherwise inactive.

Detailed technical analysis of the "Code Red" worm can be found in CA-2001-19.

II. Impact

Data reported to the CERT/CC indicates that the "Code Red" worm infected more than 250,000 sytems in just 9 hours. Figure 1 illustrates the activity between 6:00 AM EDT and 8:00 PM EDT on July 19, 2001.

NOTE: After 8:00 PM EDT on July 19 (0:00 GMT July 20), the worm switched into flood mode on most infected systems, so the number of infected systems remained fairly constant after that time.

Our analysis estimates that starting with a single infected host, the time required to infect all vulnerable IIS servers with this worm could be less than 18 hours. Since the worm is programmed to continue propagating for the first 19 days of the month, widespread denial of service may result due to heavy scan traffic.

As reported in CA-2001-19, infected systems may experience web site defacement as well as performance degradation as a result of the propagating activity of this worm. This degradation can become quite severe, and in fact may cause some services to stop entirely, since it is possible for a machine to be infected with multiple copies of the worm simultaneously.

Furthermore, it is important to note that the IIS indexing vulnerability that the "Code Red" worm exploits can be used to execute arbitrary code in the Local System security context. This level of privilege effectively gives an attacker complete control of the infected system.

III. Solutions

The CERT/CC encourages all Internet sites to review CA-2001-13 and ensure workarounds or patches have been applied on all affected hosts on your network.

If you believe a host under your control has been compromised, you may wish to refer to

> Steps for Recovering from a UNIX or NT System Compromise

Known versions of the worm reside entirely in memory; therefore, a reboot of the machine will purge the worm from the system. However, due to the rapid propagation of the worm, the likelihood of re-infection is quite high. Taking the system offline and applying the vendor patch will eliminate the vulnerability exploited by the "Code Red" worm.

IV. Good Practices

Consistent with the security best-practice of denying all network traffic and only selectively allowing that which is required, ingress and egress filtering should be implemented at the network edge. Likewise, controls must be in place to ensure that all software used on a network is properly maintained.

Ingress filtering

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. Servers are typically the only machines that need to accept inbound connections from the public Internet. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound connections to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound connections to non-authortized services. In this fashion, the effectiveness of many intruder scanning techniques can be dramatically reduced. With "Code Red," ingress filtering will prevent instances of the worm outside of your network from infecting machines in the local network that are not explicitly authorized to provide public web services. Cisco has published a tech tip specifically addressing ingress filtering for the "Code Red" worm at

> http://www.cisco.com/warp/public/63/nbar_acl_codered.shtml.

Egress filtering

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound connections to the Internet. In the case of "Code Red," employing egress filtering will prevent compromised IIS servers on your network from further propagating the worm.

Installing new software with the latest patches

When installing an operating system or application on a host for the first time, it is insufficient to merely use the install media. Vulnerabilities are often discovered after the software becomes widely distributed. Thus, prior to connecting this host to the network, the latest security patches for the software should be obtained from the vendor and applied.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Cisco Systems

Cisco has published a security advisory describing this vulnerability at

> http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

Microsoft Corporation

The following document regarding the vulnerability exploited by the "Code Red" worm is available from Microsoft:

> http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

---

Author(s): Roman Danyliw and Allen Householder

Revision History

```
Jul 26, 2001: Initial release
Jul 30, 2001: Added link to Polish translation
Aug 16, 2001: Added link to Cisco ingress filtering tech tip, updated link to Microsoft cumulative patch
Aug 23, 2001: Updated contact information
Jan 17, 2002: Updated feedback link
```