Xerox Document Centre

DC Tips

... for the user

dc01cc0253
November 8, 2002

Impact of Internet Worm Variants on Document Centres

Purpose

This document describes the impact of the **Code Red**, **Code Blue, Code Green** and **Nimda** worms on the Document Centre family of products. You can find a detailed technical review of the Code Red worm and it's functionality in the references section at the end of this document (reference number 1). The Code Blue and Green worms are functionally different programs, but attack similar vulnerabilities in the Web server. The Document Centre is immune to Code Blue and Green for the same reasons the Document Centre is immune to Code Red.

Overview of the Code Red Worm

The Code Red worm seeks to infect Web servers running Microsoft Internet Information Server. The worm uses a vulnerability of a buffer overrun in the URL input processing function of the IDQ.DLL library. The Internet Information Server software then allows the worm to inject its instruction set into the active memory of the server. When running on the server, the program moves through several modes of operation, one of which is designed to propagate the code through infection of other hosts. Because the worms discussed in this document use this vulnerability to attack, this document treats them as one method of attack.

A side effect of the worm attack is exposure of unexpected problems on devices with embedded Web servers listening to TCP port 80. Some of these problems include device crashes.

This document applies to these Xerox products:

	DC 555/545/535 ST
x	DC 490/480/470/460 ST
x	DC 440/432/425/420 ST
x	DC 340/332 ST
x	DC 265/255/240 ST/LP
x	DC 230/220 ST/LP
x	DCCS 50

Overview of the Code Blue Worm

The Code Blue worm seeks to infect Web servers running Microsoft Internet Information Server. The worm uses known vulnerabilities and a vulnerability in "folder traversal" to inject code into active memory. This worm uses a carefully constructed URL to exploit the folder traversal problem and gain elevated privileges.

Overview of the Code Green Worm

The Code Green worm uses the same method as Code Red to infect servers. Reports describe the Code Green worm as one that attempts a remote system patch by infecting a host, removing the Code Red worm and patching the operating system to prevent future infections.

Overview of the Nimda Worm

The Nimda worm infects servers and workstations much the same way as the Code Red variants. This worm is particularly dangerous because it also spreads by infecting open Guest shares and as email attachments. Email recipients that open infected attachments infect their workstations, and enhance the worm's impact on the community. The Document Centre does not receive email, nor does it have open Guest shares, making the device immune to the Nimda worm. In addition, the Nimda worm infects a device using the same method described for the other worms with the same impact to the Document Centre.

Risk to the Document Centre

While the worm probes systems based solely on their IP address, it only infects systems with the vulnerabilities mentioned above. The Document Centre does not run Microsoft Internet Information Server, and therefore is not vulnerable to the buffer overrun in the attack.

When the worm attacks a Document Centre, the Document Centre filters the initial request that contains the buffer overrun attack and parses it for useable data. The attack is launched as a GET request with a "/default.ida" parameter. Since this file does not exist on the Document Centre, it returns the appropriate HTML 404 error for "file not found" and immediately terminates the session at the TCP level without processing the remainder of the request.

Furthermore, the Document Centre cannot execute the code delivered in the attack because it uses and seeks functions and instruction sets specific to the Win32 model of programming. The Win32 model is used by Microsoft Windows 95, 98, ME, NT, 2000 and XP. The Document Centre does not use the Win32 model, so applications that use it cannot execute on the Document Centre.

Impact on the Document Centre

The only impact to the Document Centre, as a consequence of repeated attacks, is the overhead required to generate and emit the HTML 404 error messages. The Document Centre may, in the extreme case, experience a brief slow down in document processing and pages printed when processor time is sacrificed by producing error messages.

The nature of the attack ensures that this worm probes a Document Centre only once each instance, so the total number of hits in a given day remains small. Average user access to the Web interface generally generates a greater number of hits.

Software Tested

The attack was repeated using these software versions.

DC220	ESS 1.12.47.1
DC230	ESS 1.12.18
DC230	ESS 1.12.35.1
DC230	ESS 1.12.50
DC230	ESS 1.12.68
DC332	ESS 1.12.69
DC340	ESS 1.12.35.1s
DC432	ESS 2.2.11
DC440	ESS 2.2.6
DC440	ESS 2.3.1
DC440	ESS 3.0.5.3
DC265	ESS 18.6.73.1
DC265	ESS 18.6.67.1
DC460	ESS 19.01.506.1
DC460	ESS 19.01.511.2
DC470	ESS 19.01.508.2
DC480	ESS 19.02.050.1
DC490	ESS 19.02.050.1
DCCS50	system software 158

Technical Notes Related to the Attack

The following process gives a brief description of the worm's (or variant's) pattern of execution.

System Invasion

1. The worm obtains the local IP address of the vulnerable device to use later for propagation.
2. The worm determines the local system language.
3. The worm checks to see if the virus has already executed on the local system. If not, it continues with step 4 of this process. If it has executed, it moves on to the activity described in the "Propagation" portion of this process.
4. The worm sets the thread count to 600 for Chinese/Taiwanese systems, 300 for all other systems.
5. The worm creates new propagation threads up to the 300 or 600 count threshold. This means that either 300 or 600 threads are working simultaneously in attempts to propagate the virus to other devices.

6. After the threads are spawned, the worm sleeps for one day (non-Chinese systems) or two days (Chinese systems), and then reboots Windows.

Propagation

7. Based upon the IP address (step 1), the worm builds a table of "intended targets" using an IP mask and adding random numbers to the local IP address. Each of the threads (step 5) target an IP address in this table.
8. The worm attempts an HTTP connection to the first entry in the "intended targets" list of IP addresses. If the connection is established, the virus attempts to upload a copy of itself to the target device. Three possible outcomes of this attempt may occur:
   - The targeted system accepts the uploaded virus, propagation is successful, and the new virus activates.
   - The targeted system crashes, unable to process the attempted connection request. Certain versions of HP Jet Direct Firmware exhibit this behavior.
   - The targeted system sees the connection request as invalid, and closes the connection. The Document Centre takes this action.

References

If you have further inquiries, you may contact your Xerox Customer Support Center and/or use these references:

- http://www.eeye.com/html/Research/Advisories/AL20010804.html - eEye Digital Security analysis
- http://www.incidents.org/react/code_redII.php - SANS Incident Report
- http://www.unixwiz.net/techtips/CodeRedII.html - Software Consulting Central analysis
- http://forums.itrc.hp.com/cm/QuestionAnswer/1,1150,0x93a772234586d5118ff00090279cd0f9,00.html - HP discussion group noting behavior of J3111A Firmware G.05.35
- http://www.microsoft.com/technet/security/bulletin/ms01-033.asp?frame=true - Microsoft Security Bulletin MS01-033

Additional Information

Xerox Document Centre Technical Support Organization welcomes feedback on all DC Tips documentation - send feedback via e-mail to: USA.DSSC.Doc.Feedback@mc.usa.xerox.com.

Other DC Tips are available at the following URL: http://www.xerox.com/DocumentCentreFamily/Tips.

THE DOCUMENT COMPANY
XEROX®