CERT Incident Note IN-2001-10: "Code Red" Worm Crashes IIS 4.0 Servers with URL Redirection Enabled

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

"Code Red" Worm Crashes IIS 4.0 Servers with URL Redirection Enabled

Release Date: August 16, 2001

Systems Affected

- Microsoft Windows NT 4.0 running Internet Information Server (IIS) 4.0 with URL Redirection enabled

I. Overview

The CERT/CC has received numerous reports of Windows NT 4.0 IIS 4.0 servers patched according to Microsoft Security Bulletin MS01-033 crashing when scanned by the "Code Red" worm.

II. Description

A vulnerability in Microsoft IIS 4.0 allows an attacker to crash an IIS 4.0 server by sending a crafted URL if the server is configured to use URL redirection (URL redirection is not enabled by default). This vulnerability is exercised by the "Code Red" worm, but it is distinct from the vulnerability described in CA-2001-13 that allows the worm to compromise systems. IIS 4.0 servers configured to use URL redirection and patched according to Microsoft Security Bulletin MS01-033 are no longer vulnerable to compromise by the "Code Red" worm, but they may crash due to this new vulnerability.

For more information, please see

CERT Vulnerability Note VU#544555 - Microsoft Internet Information Server 4.0 (IIS) vulnerable to DoS when URL redirecting is enabled

Microsoft Security Bulletin MS01-044

III. Impact

"Code Red" scanning activity can result in a denial-of-service attack against a Windows NT 4.0 IIS 4.0 server with URL redirection enabled.

IV. Solutions

Apply the patch from Microsoft Security Bulletin MS01-044.

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32061

V. Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are affected by this activity, please send mail to cert@cert.org.

Author(s): Brian B. King