

Using Cisco Secure IDS/NetRanger Custom String Match Signatures for "Code Red" Worm Remote Buffer Overflow in Microsoft Index Server ISAPI Extension in IIS 4.0 and 5.0

Document ID: 13870

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Custom String Match Signatures

- Signature 1 Index Server Access with Attempted Exploitation

- Signature 2 Index Server Access Buffer Overflow "Code Red" Worm

Related Information

Introduction

As of the end of July 2003, Computer Economics (an independent research organization in Carlsbad, CA) estimated that the "Code Red" worm had cost corporations \$1.2 billion (U.S.) in recovery from network damage and in lost productivity. This estimate rose significantly with the subsequent release of the more potent "Code Red II" worm. The Cisco Secure Intrusion Detection System (IDS), a key component of the Cisco SAFE Blueprint, has demonstrated its value in detecting and mitigating network security risks, including the "Code Red" worm.

This document describes a software update to detect the exploitation method used by the "Code Red" worm (see Signature 2 below).

You can create the custom string match signatures shown below to catch the exploitation of a buffer overflow for web servers running Microsoft Windows NT and Internet Information Services (IIS) 4.0 or Windows 2000 and IIS 5.0. Note also that the indexing service in Windows XP beta is also vulnerable. The security advisory that describes this vulnerability is at <http://www.eeye.com/html/Research/Advisories/AD20010618.html> . Microsoft has released a patch for this vulnerability that can be downloaded from <http://www.microsoft.com/technet/security/bulletin/MS01-033.msp> .

The signatures discussed in this document became available in signature update release S(5). Cisco Systems recommends that sensors be upgraded to 2.2.1.8 or 2.5(1)S3 signature update prior to implementing this signature. Registered users can download these signature updates from the Cisco Secure Software Center. All users can contact Cisco Technical Support by e-mail and telephone through the Cisco Worldwide Contacts.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the following software versions:

- Microsoft Windows NT and IIS 4.0
- Microsoft Windows 2000 and IIS 5.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Custom String Match Signatures

There are two specific custom string match signatures to address this issue. Each signature is described below, and applicable product settings are provided.

Signature 1 Index Server Access with Attempted Exploitation

This signature fires on an attempted buffer overflow on the Indexing Server ISAPI Extension combined with an attempt to pass shell code to the server to gain privileged access in the original form of the code. The signature fires only on the attempt to pass shell code to the target service in an attempt to gain full SYSTEM level access. One possible problem is that this signature does not fire if the attacker does not try to pass any shell code, but just runs the buffer overflow against the service in an attempt to crash IIS and create a denial of service.

String

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

Product Settings

- Occurrences: 1
- Port: 80

Note: If you have web servers listening on other TCP ports (for example, 8080), you need to create a separate custom string match for each port number.

- Recommended Alarm Severity Level:
 - ◆ High (Cisco Secure Policy Manager)
 - ◆ 5 (Unix Director)
- Direction:

TO

Signature 2 Index Server Access Buffer Overflow "Code Red" Worm

The second signature fires on an attempted buffer overflow on the Indexing Server ISAPI Extension combined with an attempt to pass shell code to the server to gain privileged access in the obfuscated form that

the "Code Red" Worm uses. This signature fires only on the attempt to pass shell code to the target service in an attempt to gain full SYSTEM level access. One possible problem is that this signature does not fire if the attacker does not try to pass any shell code, but just runs the buffer overflow against the service in an attempt to crash IIS and create a denial of service.

String

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

Note: There are no blank spaces in the above string.

Product Settings

- Occurrences: 1
- Port: 80

Note: If you have web servers listening on other TCP ports (for example, 8080), you need to create a separate custom string match for each port number.

- Recommended Alarm Severity Level:
 - ◆ High (Cisco Secure Policy Manager)
 - ◆ 5 (Unix Director)
- Direction:

TO

For more information on Cisco Secure IDS, refer to Cisco Secure Intrusion Detection.

Related Information

- [Technical Support Routers](#)
- [Cisco Security Advisories](#)
- [Cisco Secure Intrusion Detection Support Page](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 24, 2008

Document ID: 13870
