使用" Code Red "蠕虫远程缓冲溢出的Cisco Secure IDS/NetRanger自定义串匹配签名在Microsoft Index服务器在IIS 4.0和5.0的ISAPI扩展名

Contents

Introduction

自底2003年7月，计算机经济(一个独立研究组织在卡尔斯巴德， CA)估计" Code Red "蠕虫开销了公司$1.2十亿(美国)在从网络损伤的恢复和在丢失的生产率。此估计用更加有力的“红色代码II”蠕虫的后续版本大量增加。Cisco安全入侵监测系统(IDS)， Cisco SAFE图纸的一个关键组件，展示了其在发现的值和缓和网络安全风险，包括" Code Red "蠕虫。

本文描述一次软件更新发现" Code Red "蠕虫的开发使用的方法(请参阅下面的签名2)。

您能创建如下所示的自定义串匹配签名捉住一缓冲区溢出的开发管理微软Windows NT和互联网信息服务(IIS)的Web服务器的4.0或Windows 2000和IIS 5.0。也注意在β的Windows XP的索引服务也易受攻击。描述此弱点的安全建议在 http://www.eeye.com/html/Research/Advisories/AD20010618.html 。Microsoft发布了可以从 http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx下载的此弱点的一个补丁程序 。

在本文讨论的签名变得可用在签名更新版本S(5)。Cisco系统建议传感器被升级到2.2.1.8或2.5(1)S3签名更新在实现此签名之前。注册的用户能从Cisco安全软件中心下载这些签名更新。所有用户能由电子邮件与Cisco技术支持和电话联系通过Cisco全球联络。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息基于以下软件版本：

- 微软Windows NT和IIS 4.0
- Microsoft Windows 2000和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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

自定义串匹配签名

有解决此问题的两个特定自定义串匹配签名。每个签名下述，并且提供可适用的产品设置。

签名1 —与试图非法的索引服务器访问

在一尝试的缓冲区溢出的此签名火在与尝试一起的索引服务器ISAPI扩展通过shell代码到服务器获取特许访问以代码的原来形状。签名仅火在尝试通过shell代码到目标服务为获得充分的系统层使用。一个可能的问题是此签名不射击，如果攻击者不设法通过任何shell代码，但是执行缓冲区溢出服务为失败IIS和创建拒绝服务。

字符串

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

产品设置

- 出现时间：1
- 端口：80

Note: 如果有Web服务器监听在其他TCP端口的(例如， 8080)，您需要创建每端口号的一个单独的自定义字串匹配。

- 级的推荐的告警严重性：高(Cisco Secure Policy Manager)5 (Unix导向器)
- 方向：

签名2 —索引服务器访问缓冲区溢出" Code Red "蠕虫

在一尝试的缓冲区溢出的第二签名火在与尝试一起的索引服务器ISAPI扩展通过shell代码到服务器获取特许访问以" Code Red "蠕虫使用的被弄暗淡的形式。此签名在尝试仅射击通过shell代码到目标服务为获得充分的系统层使用。一个可能的问题是此签名不射击，如果攻击者不设法通过任何shell代码，但是执行缓冲区溢出服务为失败IIS和创建拒绝服务。

字符串

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

Note: 没有在上述字符串的空格。

产品设置

- 出现时间：1
- 端口：80

Note: 如果有Web服务器监听在其他TCP端口的(例如， 8080)，您需要创建每端口号的一个单独的自定义字串匹配。

- 级的推荐的告警严重性：高(Cisco Secure Policy Manager)5 (Unix导向器)
- 方向：

关于Cisco Secure IDS的更多信息，请参见Cisco安全入侵检测。

Related Information

- 技术支持–路由器
- Cisco安全建议
- Cisco安全入侵检测支持页
- Technical Support - Cisco Systems