使用 Cisco Secure IDS/NetRanger 自定义字符串匹配签名抵御“红色代码”蠕虫在 IIS 4.0 和 5.0 Microsoft Index Server ISAPI Extension 中导致的远程缓冲溢出

目录

简介

自七月结尾2003年，计算机经济(一个独立研究组织在卡尔斯巴德， CA)预计" Code Red "蠕虫病毒开销了公司$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”蠕虫病毒的后续版本大量增加。Cisco安全入侵监测系统(IDS)， Cisco SAFE图纸的关键组件，展示了其在检测的值和缓和网络安全风险，包括" Code Red "蠕虫病毒。

本文描述软件更新由" Code Red "蠕虫病毒检测开发使用的方法(请参阅下面的签名2)。

您能创建如下所示的自定义字符串匹配签名捉住一缓冲区溢出的开发运行微软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Windows XP beta的索引服务也易受攻击。描述此漏洞的安全建议在 http://www.eeye.com/html/Research/Advisories/AD20010618.html 。Microsoft发布可以从 http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx下载的此漏洞的一补丁程序 。

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

先决条件

要求

本文档没有任何特定的要求。

使用的组件

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

自定义字符串匹配签名

有解决此问题的两个特定自定义字符串匹配签名。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

在一已尝试缓冲区溢出的此签名火在索引服务器ISAPI扩展结合了以尝试通过shell代码到服务器获得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全双工系统层使用。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：1
- 波尔特：80

注意： 如果有Web服务器侦听在其他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：海伊(Cisco Secure Policy Manager)5 (UNIX向导)
- 方向：

签名2 —索引服务器访问缓冲溢出" Code Red "蠕虫病毒

在一已尝试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代码到服务器获得特许访问以" Code Red "蠕虫病毒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全双工系统层使用。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
```

注意： 没有在上述字符串的空格。

产品设置

- 出现：1
- 波尔特：80

注意： 如果有Web服务器侦听在其他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：海伊(Cisco Secure Policy Manager)5 (UNIX向导)
- 方向：

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

相关信息

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