如何在 Cisco缓存和 内容引擎中过滤红色代码

目录

简介

本文在过滤提供信息在Cisco Cache和内容引擎的红色代码蠕虫。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

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。

配置

本部分提供有关如何配置本文档所述功能的信息。

配置

当尝试连接到不存在的站点时，许多透明缓存被淹没。本文提供一解决方案过滤能影响思科缓存解决方案的红色代码蠕虫。红色代码在互联网信息服务器(IIS)的一份default.ida脚本使用缓冲区溢出检测安全漏洞代码。红色代码使用此超文本传输协议(HTTP)请求：

```
get http://random-ip-address/default.ida?long-string-of-data
```

从以上示例的是缓冲区溢出和指令代码蠕虫病毒的。您能过滤此通过使用使用a url-regex匹配内容的分块规则。对于Cisco缓存引擎硬件运行CE2.XX软件和运行2.XX或3.XX软件的Cisco内容引擎硬件，请配置如下：

```
rule enable
rule block url-regex ^http://.*/default\.ida$
rule block url-regex ^http://.*www\.worm\.com/default\.ida$
```

发出**show rule all命令**显示累计此分块规则命中数的数量。对于运行3.XX软件的内容引擎硬件，您能是更多特定和不拒绝请求，但是重写到一本地Web服务器表明您的站点被传染。请使用一个规则类似于这一个：

```
rule enable
rule rewrite url-regsub ^http://.*/default\.ida$ http://local-webserver/codered.html
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 内容网络产品支持
- Cisco缓存引擎3.0软件下载(仅限注册用户)
- Cisco缓存引擎2.0软件下载(仅限注册用户)
- 技术支持 - Cisco Systems