Cisco AsyncOS 8.0.8 for Web 版本说明

本文档累积了针对所有思科网络安全设备 AsyncOS 8.0.x 版本的说明信息。

发布日期：2014 年 1 月 27 日

修订日期：2016 年 7 月 18 日

目录

此版本中的新增功能

版本 8.0.8 (GD) 中的新增功能

此版本的重大更改与禁用和启用 SSLv3 和临时椭圆曲线 Diffie-Hellman (ECDHE) 功能相关。

注意 请将 Cisco AsyncOS for Web 用户指南 v8.0.6 与此版本结合使用。

功能	说明
SSL 配置	为获得增强的安全性，可以对多个服务启用和禁用 SSLv3。在禁用 SSLv3 的情况下，服务会使用 TLSv1.0。 您可以对设备管理 Web 用户界面、代理服务（包括安全客户端的 HTTPS 代理和凭据加密）、安全 LDAP 服务（包括身份验证、外部身份验证、SaaS SSO 和安全移动）以及更新服务启用或禁用 SSLv3。 使用 Web 界面（“系统管理”(System Administration) > “SSL 配置”(SSL Configuration)）或 CLI (`sslconfig`)。

ECDHE 身份验证	在后续版本中，会支持额外的 ECDH 密码功能；但是，一些额外密码所附带的某些指定曲线会导致设备在安全 LDAP 身份验证和 HTTPS 流量解密时关闭连接。
	如果遇到这些问题，请执行 `sslconfig` 命令和 `ECDHE` 选项命令，为其中一个或两个功能禁用或启用 ECDHE 密码功能。以下为此命令的部分 CLI 内容：
	`Choose the operation you want to perform:`
	`- SSLV3 - Enable or disable SSL v3.`
	`- ECDHE - Enable or disable ECDHE Authentication.`
	`[]> ECDHE`
	
	`ECDHE cipher status is enabled in Proxy & enabled in LDAP`
	
	`Please select an option to change ECDHE cipher status:`
	`- 1 - Toggle ECDHE cipher status in Proxy`
	`- 2 - Toggle ECDHE cipher status in LDAP`
	`- 3 - Enable ECDHE cipher in both Proxy & LDAP`
	`- 4 - Disable ECDHE cipher  in both Proxy & LDAP`
	`[]>`

版本 8.0.7 中的新增功能

此版本属于维护版本，因此并未增加新功能。

版本 8.0.6 中的新增功能

此版本的所有新功能均与文件信誉和文件分析功能相关。

功能	说明
判定更新报告变更	现在点击判定更新报告中的 SHA-256 链接之后，会在 Web 跟踪中显示所有包含该 SHA-256 的可用事务。
信誉得分阈值自定义	您可以采用一个自定义值取代云提供的高级恶意软件防护信誉阈值。
SSL 证书检索	AsyncOS 会自动获取最新的 SSL 证书。
支持端口 443	现在可支持端口 443，用于高级恶意软件防护文件信誉查询。
代理支持	设备现在可通过上游代理与云信誉服务通信。您可在“高级恶意软件防护”(Advanced Malware Protection) 设置中的“高级”(Advanced) 部分对此进行配置。 说明：该设备当前不支持通过代理与文件分析服务器连接。
改进了高级恶意软件防护的日志记录	AsyncOS 将 文件分析故障记录在 AMP 日志中。

版本 8.0.5 中的新增功能

功能	说明
文件信誉过滤和文件分析	高级恶意软件防护 (AMP) 是一个附加的许可功能，所有思科网络安全设备客户均可使用。AMP 是一个综合性恶意软件防护解决方案，它支持恶意软件检测与拦截、持续分析和追溯性警报等功能。它充分利用了思科庞大的云安全情报网络。 提供增强的文件信誉功能、详细的文件行为报告、持续的文件分析，以及追溯性判定警报，AMP 对思科网络安全设备中已支持的防恶意软件检测和拦截功能进行了完善。 有关需求和其他详细信息，请参阅联机帮助或《用户指南》中的“文件信誉过滤和文件分析”章节。

版本 8.0.0 中的新增功能

功能	说明
新功能	
云网络安全连接器	此版本引入新的配置模式，通过该配置模式，您可连接并将流量定向到思科云网络安全以进行策略实施和威胁防御。 云网络安全连接器模式可通过思科网络安全虚拟设备和物理网络安全设备使用。 关于云连接器的文档在《用户指南》第 3 章“将设备连接到云网络安全塔”。要使网络安全设备在云连接器模式下工作，首先应“配置云连接器”。 **注意** 云连接器模式不支持 Kerberos 身份验证和 IPv6 地址。 **注意** 升级到此版本后，如果您计划在云连接器模式下使用设备，请勿使用系统安装向导将设备置于标准模式。请将设备直接置于云连接器模式。
Kerberos 身份验证	Kerberos 是一个适用于 Windows、Mac OS X 和其他操作系统的“穿越式”身份验证协议。由于现在许多操作系统不再支持 NTLM 或 NTLM SSO，Kerberos 已成为非常普遍的身份验证协议。此功能支持 Kerberos 版本 5（MS KRB5 和 KRB5）和 AD 服务器（例如 2003、2008、2008R2 和 2012）。我们还支持以下网络浏览器：IE、Chrome、Firefox 和 Safari。 **注意** 在此版本之前创建的 Active Directory 域没有可用的 Kerberos 方案。

功能	说明
思科网络安全虚拟设备	思科网络安全设备作为一个虚拟机可托管到您的自有网络。 对于从思科购买的虚拟设备，需要单独的许可证，以及运行 VMware ESXi 4.x、5.0 或 5.1的思科 UCS 服务器（刀片式或机架式）硬件平台。 《思科安全虚拟设备安装指南》中包含关于虚拟设备要求的详细信息。 新网络安全虚拟设备模式和配置如下： • S000V （250 GB 磁盘空间、50 GB 缓存空间、1 核 CPU、4 GB 内存） • S100V （250 GB 磁盘空间、50 GB 缓存空间、2 核 CPU、6 GB 内存） • S300V （1024 GB 磁盘空间、200 GB 缓存空间、4 核 CPU、8 GB 内存） 此功能包括对用于网络安全设备的 Web AsyncOS 进行的以下更改: • 通过思科网络安全虚拟设备许可证，您可在网络中克隆和运行多个虚拟设备。 • 安装虚拟设备许可证的 loadlicense CLI 命令。 • 您可以在多个虚拟设备上使用同一许可证。 功能密钥包含在虚拟设备许可证中。功能密钥将和许可证同时到期。购买新的功能密钥需要下载并安装新的虚拟设备许可证。 因为功能密钥包含在虚拟设备许可证中，所以 AsyncOS 功能没有 30 天评估期。 安装虚拟设备许可证之后，才能开启“技术支持”通道。 版本和 supportrequest CLI 命令也已更新为包括虚拟设备的信息。 对于配置错误的虚拟设备，将出现新的警报和日志。 有关详细信息，请参阅部署虚拟设备（第 10 页）。
IPv6 支持	显式和透明部署模式均支持 IPv6。IPv6 功能拥有与 IPv4 同样熟悉的配置界面。现有功能（包括 HTTP/HTTPS/FTP、L4TM、代理旁路、URL 分类、AVC 等）均支持 IPv6。日志和报告基本保持不变，但对 IPv6 流量提供额外的可视性。 有关其他信息，请参阅 IPv6 地址的功能支持。

功能	说明
增强	
用户界面	AsyncOS 8.0.0 引入更加易用的界面，支持“拖放”功能。通过“查看报告”页面、收藏夹页面和其他界面，用户可拖放屏幕上的项目进行重新排序，例如进行列表排序或将报告控制面板的组件移动到不同位置。 以下页面支持拖放功能： • 标识 • 访问策略 • 解密策略 • 路由策略 • 思科数据安全 • 出站恶意软件扫描 • 外部数据丢失预防 另外： • 用户现在可以创建自己的收藏夹，对“我的报告”(My Reports) 进行自定义和安排。可以通过“我的收藏夹”(My Favorites) 菜单实现这些功能。 • 用户现在可使用 Web 界面或命令行界面，分别调整 Web 信誉和分类设置。 • 在重置配置时，用户可以选择保留网络设置。

升级路线

升级到版本 8.0.8-113

要确保成功升级，请按照升级前要求（第 8 页）和安装和升级说明（第 8 页）中描述的升级流程做好升级准备。

您可以将思科网络安全设备 AsyncOS 从以下版本升级至版本 8.0.8-113：

- 7-5-0-703
- 7-5-0-727
- 7-5-0-810
- 7-5-0-825
- 7-5-0-833
- 7-5-0-834
- 7-5-0-836
- 7-5-0-838
- 7-5-0-840
- 7-5-0-850
- 7-5-0-860
- 7-5-0-861
- 7-5-1-074
- 7-5-1-079
- 7-5-1-085
- 7-5-1-201
- 7-5-1-223
- 7-5-1-230
- 7-5-1-245
- 7-5-2-118
- 7-5-2-202
- 7-5-2-303
- 7-5-2-304
- 7-5-2-322
- 7-5-2-501
- 7-5-7-048
- 7-7-0-500
- 7-7-0-608
- 7-7-0-706
- 7-7-0-710
- 7-7-0-725
- 7-7-0-736
- 7-7-0-744
- 7-7-0-753
- 7-7-0-757
- 7-7-0-760
- 7-7-0-761
- 7.7.5-190
- 7.7.5-194
- 7.7.5-195
- 7.7.5-302
- 7.7.5-311
- 8-0-0-408
- 8-0-0-503
- 8-0-5-075
- 8-0-5-079
- 8-0-5-082
- 8-0-6-053
- 8-0-6-078
- 8-0-6-081
- 8-0-6-101
- 8-0-6-119
- 8-0-6-121
- 8-0-6-142
- 8-0-7-142

升级到版本 8.0.7-142

要确保成功升级，请按照升级前要求（第 8 页）和安装和升级说明（第 8 页）中描述的升级流程做好升级准备。

您可以将思科网络安全设备 AsyncOS 从以下版本升级至版本 8.0.7-142：

- 7-5-0-703
- 7-5-0-727
- 7-5-0-810
- 7-5-0-825
- 7-5-0-833
- 7-5-0-834
- 7-5-0-836
- 7-5-0-838
- 7-5-0-840
- 7-5-0-850
- 7-5-0-860
- 7-5-0-861
- 7-5-1-074
- 7-5-1-079
- 7-5-1-085
- 7-5-1-201
- 7-5-1-223
- 7-5-1-230
- 7-5-1-245
- 7-5-2-118
- 7-5-2-202
- 7-5-2-303
- 7-5-2-304
- 7-5-2-322
- 7-5-2-501
- 7-5-7-048
- 7-7-0-500
- 7-7-0-608
- 7-7-0-706
- 7-7-0-710
- 7-7-0-725
- 7-7-0-736
- 7-7-0-744
- 7-7-0-753
- 7-7-0-757
- 7-7-0-760
- 7-7-0-761
- 7.7.5-190
- 7.7.5-194
- 7.7.5-195
- 7.7.5-302
- 7.7.5-311
- 8-0-0-408
- 8-0-0-503
- 8-0-5-075
- 8-0-5-079
- 8-0-5-082
- 8-0-6-053
- 8-0-6-078
- 8-0-6-101
- 8-0-6-119

升级前要求

更新 RAID 控制器固件

在升级 AsyncOS 软件之前，请按*思科 RAID 控制器固件更新（仅限 S360/S370/S660/S670，要求重启）版本说明*所述更新 RAID 控制器固件。

登录到管理员帐户

您必须以管理员身份登录才能执行升级。

保留系统容量报告中的升级前数据

关于 Web 信誉 和 Web 分类的 CPU 使用率的升级前数据（如系统容量报告页面中各功能的 CPU 使用率表所示）在升级后将不可用。如果需要保留此历史数据，请在升级之前将各功能的 CPU 使用率表数据导出或另存为 CSV 或 PDF 文件。

在此版本中，Web 信誉和 Web 分类数据合并为名为“可接受的使用和信誉”的单个比较分析。

已知问题

在您升级 Web AsyncOS 前，请参阅“有关已知和已解决问题的最新信息”一节，第 15 页。

安装和升级说明

兼容性详细信息

与思科安全管理 AsyncOS 的兼容性

有关此版本和思科内容安全管理 AsyncOS 版本之间的兼容性信息，请参阅兼容性表格：http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html。

IPv6 和 Kerberos 在云连接器模式下不可用

当在云连接器模式下进行设备配置时，IPv6 地址和 Kerberos 身份验证的不可用选项会在 Web 界面的页面上显示。虽然这些选项看似可用，但它们在云连接器模式下不受支持。在云连接器模式下，请勿尝试配置设备使用 IPv6 地址或 Kerberos 身份验证。

IPv6 地址的功能支持

支持 IPv6 地址的特性和功能：

- 命令行和 Web 界面。您可使用 http://[2001:2:2::8]:8080 或 https://[2001:2:2::8]:8443 访问 WSA
- 对 IPv6 数据流量 (HTTP/HTTPS/SOCKS/FTP) 执行代理操作
- IPv6 DNS 服务器
- WCCP 2.01（Cat6K 交换机）和第 4 层透明重定向
- 上游代理
- 身份验证服务
  - Active Directory（NTLMSSP、Basic 和 Kerberos）
  - LDAP
  - SaaS SSO
  - 通过 CDA（WSA 和 CDA 之间仅支持通过 IPv4 协议进行通信）的透明用户标识
  - 凭据加密
- Web 报告和 Web 跟踪
- 外部 DLP 服务器（WSA 和 DLP 服务器之间仅支持通过 IPv4 协议进行通信）
- PAC 文件托管

需要 IPv4 地址的特性和功能：

- 内部 SMTP 中继 (Internal SMTP Relay)
- 外部身份验证
- 日志订阅推送方法：FTP、SCP 和系统日志
- NTP 服务器
- 本地更新服务器，包括用于更新的代理服务器
- 身份验证服务
- AnyConnect 安全移动
- Novell eDirectory 身份验证服务器
- 最终用户通知页面的自定义徽标
- 网络安全设备和安全管理设备之间的通信
- 版本 2.01 之前的 WCCP 版本
- SNMP

Kerberos 身份验证对于操作系统和浏览器的的可用性

您可以在以下操作系统和浏览器中使用 Kerberos 身份验证功能：

- Windows Server 2003、2008、2008R2 和 2012
- Mac （OSX 10.5+ 版本）的 Safari 和 Firefox 浏览器的最新版本
- Windows 7 和 XP 的 IE （7+ 版本）和 Firefox 与 Chrome 浏览器的最新版本

Kerberos 身份验证对于以下操作系统和浏览器不适用：

- 前面未提到的 Windows 系统
- 前面未提到的浏览器
- iOS 和 Android

部署虚拟设备

要部署虚拟网络安全设备，请参阅*思科内容安全虚拟设备安装指南*，可从 http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html 获取。

从硬件设备迁移到虚拟设备

将您的配置从物理硬件迁移：

步骤 1 将您的硬件设备升级至此 AsyncOS 版本。

步骤 2 保存配置文件。

步骤 3 根据此 AsyncOS 版本设置虚拟设备。

步骤 4 将配置文件从您的硬件设备导入到虚拟设备。

配置文件

当您从 Web 界面或命令行界面 (CLI) 升级 Web AsyncOS 时，配置保存在 /configuration/upgrade 目录下的文件中。您可以使用 FTP 客户端访问升级目录。每个配置文件名都附有版本号，而且配置文件中的密码是屏蔽的，因此人类无法识别。

通常，配置文件在不同 AsyncOS 版本间不兼容。

升级后重启

在升级 AsyncOS for Web 后，您必须重启网络安全设备。

行为变化

本节介绍在升级到最新版本后，相比 AsyncOS for Web 以前的版本，可能影响设备配置的行为变化。

X-已验证-组信头格式

由于 LDAP 身份验证和外部防数据丢失功能在设备上进行配置，AsyncOS 现在采用以下格式发送 X-已验证-组信头：

LDAP://(*LDAP server name*)/(*groupname*).

过去的格式为：LDAP://(*groupname*)。此软件变更可能要求对策略和其他依靠 X-已验证-组信头的自动化进行更改。[缺陷：CSCum91801]

升级 AsyncOS for Web

准备工作

- 执行升级前要求，包括更新 RAID 控制器固件。升级前要求（第 8 页）。

步骤 1 在“系统管理”(System Administration) > “配置文件”(Configuration File) 页面，请从网络安全设备下载保存 XML 配置文件。

步骤 2 在“系统管理”(System Administration) > “系统升级”(System Upgrade) 页面，请点击**可用的升级 (Available Upgrades)**。

刷新后，页面会显示可用的 AsyncOS for Web 升级版本列表。

步骤 3 点击**开始升级 (Begin Upgrade)** 开始升级流程。回答出现的问题。

步骤 4 升级完成后，点击**立即重启 (Reboot Now)** 可重启网络安全设备。

注意 要验证浏览器是否已在AsyncOS 的升级版本中加载了新联机帮助内容，您必须退出浏览器，然后重新打开浏览器并查看联机帮助这样做可以清除任何过时内容的浏览器缓存。

默认情况下新功能通常不会启用。

文档更新

《用户指南》和联机帮助缺失以下部分，因为在访问日志表中的 `%Xr` 描述处有一个链接指向该章节。

解释访问日志扫描判定条目

访问日志文件条目汇总并显示各个扫描引擎（例如 URL 过滤、Web 信誉过滤和防恶意软件扫描）的结果。设备在每个访问日志条目末尾的尖括号中显示此信息。

以下文本是来自访问日志文件条目的扫描判定信息。在本示例中，Webroot 扫描引擎发现恶意软件：

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",-,-,
IW_infr,-,"Trojan Phisher","-","Unknown","Unknown","-","-",489.73,0,-,[Local],"-"
,37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d
85829614fba368a421d14e64c426da5e">
```

注意 有关完整的访问日志文件条目的示例，请参阅*思科网络安全设备用户指南 AsyncOS 8.7* 第 21 页第 13 行的“访问日志文件”。

如下表所示，本示例中的每个元素与一个日志文件格式说明符对应：

位	字段值	格式说明符	说明
1	IW_infr	%XC	分配给事务的 URL 类别，缩写。当未分配类别时，此字段显示“nc”。 有关 URL 类别缩写列表，请参阅*思科网络安全设备用户指南 AsyncOS 8.7* 第 9 页第 23 行的“URL 类别说明”。
2	ns	%XW	Web 信誉过滤器得分。当出现 DNS 查找错误时，此字段将分数显示为数字、“ns”（无得分）或“dns”。
3	24	%Xv	恶意软件扫描判定 Webroot 传递到 DVS 引擎。仅适用于由 Webroot 检测到的响应。 有关更多信息，请参阅*思科网络安全设备用户指南 AsyncOS 8.7* 第 21 页第 37 行的“恶意软件扫描裁决值”。
4	“Trojan-Phisher-Gamec”	“%Xn”	与对象关联的间谍软件的名称。仅适用于由 Webroot 检测到的响应。
5	0	%Xt	与用于确定恶意软件存在几率的威胁风险比率 (TRR) 值相关联的 Webroot 特定值。仅适用于由 Webroot 检测到的响应。
6	354385	%Xs	Webroot 用作威胁标识符的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 Webroot 检测到的响应。
7	12559	%Xi	Webroot 用作跟踪标识符的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 Webroot 检测到的响应。
8	-	%Xd	恶意软件扫描判定 McAfee 传递到 DVS 引擎。仅适用于由 McAfee 检测到的响应。 有关更多信息，请参阅*思科网络安全设备用户指南 AsyncOS 8.7* 第 21 页第 37 行的“恶意软件扫描裁决值”。
9	“-”	“%Xe”	McAfee 已扫描文件的名称。仅适用于由 McAfee 检测到的响应。
10	-	%Xf	McAfee 用作扫描错误的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 McAfee 检测到的响应。
11	-	%Xg	McAfee 用作检测类型的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 McAfee 检测到的响应。
12	-	%Xh	McAfee 用作病毒类型的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 McAfee 检测到的响应。
13	“-”	“%Xj”	McAfee 已扫描病毒的名称。仅适用于由 McAfee 检测到的响应。
14	-	%XY	恶意软件扫描判定 Sophos 传递到 DVS 引擎。仅适用于由 Sophos 检测到的响应。 有关更多信息，请参阅*思科网络安全设备用户指南 AsyncOS 8.7* 第 21 页第 37 行的“恶意软件扫描裁决值”。
15	-	%Xx	Sophos 用作扫描返回代码的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 Sophos 检测到的响应。

位	字段值	格式说明符	说明
16	“-”	“%Xy”	Sophos 找到不允许内容的文件位置。对于非存档文件，此值为文件名。对于存档文件，它是存档中的对象，例如 `archive.zip/virus.exe`。仅适用于由 Sophos 检测到的响应。
17	“-”	“%Xz”	Sophos 用作威胁名称的值。在进行故障排除时，思科客户支持可能会使用该值。仅适用于由 Sophos 检测到的响应。
18	-	%Xl	思科数据安全基于思科数据安全策略的“内容”(Content) 列中的操作扫描判定。以下列表说明此字段的可能值： • **0.** 允许 • **1.** Block • **-（连字符）。**思科数据安全过滤器没有启动扫描。当思科数据安全过滤器禁用时，或者当 URL 类别操作设置为“允许”(Allow) 时，显示该值。
19	-	%Xp	基于 ICAP 响应中所给出结果的外部 DLP 扫描判定。以下列表说明此字段的可能值： • **0.** 允许 • **1.** Block • **-（连字符）。**外部 DLP 服务器没有启动扫描。当外部 DLP 扫描禁用时，或者因“外部 DLP 策略”(External DLP Policies) > “目标”(Destinations) 页面上存在免除 URL 类别而导致内容未被扫描时，显示该值。
20	`IW_infr`	%XQ	在请求端扫描过程中确定的 URL 类别判定，缩写。当 URL 过滤被禁用时，此字段列出连字符 (-)。 有关 URL 类别缩写列表，请参阅*思科网络安全设备用户指南 AsyncOS 8.7* 第 9 页第 23 行的“URL 类别说明”。
21	-	%XA	在响应端扫描过程中由动态内容分析引擎确定的 URL 类别判定，缩写。仅适用于思科网络使用控制 URL 过滤引擎。仅当动态内容分析引擎已启用，且在请求时未分配任何类别（请求端扫描判定中列出“nc”值）时才适用。 有关 URL 类别缩写列表，请参阅*思科网络安全设备用户指南 AsyncOS 8.7* 第 9 页第 23 行的“URL 类别说明”。
22	“Trojan Phisher”	“%XZ”	统一响应端防恶意软件扫描判定，不管启用了哪个扫描引擎，均提供恶意软件类别。适用于因服务器响应扫描被阻止或监控的事务。
23	“-”	“%Xk”	Web 信誉过滤器返回的威胁类型，会导致目标网站收到欠佳的信誉。通常，信誉为 -4 及更低的网站填入此字段。
24	“Unknown”	“%XO”	如果适用，应用名称由 AVC 引擎返回。仅当 AVC 引擎启用时才适用。
25	“Unknown”	“%Xu”	如果适用，应用类型由 AVC 引擎返回。仅当 AVC 引擎启用时才适用。
26	“-”	“%Xb”	如果适用，应用行为由 AVC 引擎返回。仅当 AVC 引擎启用时才适用。

位	字段值	格式说明符	说明
27	“-”	“%XS”	安全浏览扫描裁定。该值表示安全搜索或网站内容评级功能应用于事务。 有关可能值的列表，请参阅*思科网络安全设备用户指南 AsyncOS 8.7*第 9 页第 16 行的“记录成人内容访问”。
28	489.73	%XB	为满足服务请求而消耗的平均带宽，以 Kb/sec 来表示。
29	0	%XT	该值用来指示请求是否因为带宽限制控制设置而被阻止，其中“1”表示请求被阻止，“0”表示未被阻止。
30	[本地]	%l	提交请求的用户的类型：“[本地]”(Local) 或“[远程]”(Remote)。仅当 AnyConnect 安全移动启用时才适用。当它未启用时，该值是连字符 (-)。
31	“-”	“%X3”	统一请求端防恶意软件扫描判定，不管启用了哪个扫描引擎。当出站恶意软件扫描策略适用时，应用于由于客户端请求扫描而阻止或监控的事务。
32	“-”	“%X4”	该威胁名称分配至由于适用的出站恶意软件扫描策略而被阻止或监控的客户端请求。 此威胁名称与防恶意软件扫描引擎是否已启用无关。
33	37	%X#1#	来自高级恶意软件防护文件扫描的裁定： • 0：文件不是恶意的 • 1：由于其文件类型限制，文件未扫描 • 2：文件扫描超时 • 3：扫描错误 • 大于 3：文件是恶意的
34	"W32.CiscoTestVector"	%X#2#	威胁名称，根据高级恶意软件防护文件扫描来确定；“-”表示没有威胁。
35	33	%X#3#	来自高级恶意软件防护文件扫描的信誉评分。仅在云信誉服务无法确定文件的明确裁定时才使用此评分。 有关威胁评分与信誉阈值的详细信息，请参阅*思科网络安全设备用户指南 AsyncOS 8.7*的“文件信誉过滤和文件分析”第 14 章
36	0	%X#4#	上传和分析请求的指示符： “0”表示高级恶意软件防护未请求上传文件以供分析。 “1”表示高级恶意软件防护请求了上传文件以供分析。
37	"WSA-INFECTED-FILE.pdf"	%X#5#	正在下载和分析的文件的名称。
38	"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e	%X#6#	此文件的 SHA-256 标识符。

参考*思科网络安全设备用户指南 AsyncOS 8.7 的*第 21 页第 28 行的“日志文件字段和标记”的页面中关于每种格式说明符功能的说明。

有关已知和已解决问题的最新信息

使用思科缺陷搜索工具查找有关已知和已修复缺陷的最新信息。

访问思科缺陷搜索工具的要求

如果您没有思科帐户，请注册一个帐户：https://tools.cisco.com/RPF/register/register.do。

已知和已修复问题的列表

注意 之前版本中遗留的问题在此版本中仍未解决。通过搜索可以查找此版本中的新增问题和解决方法。

版本 8.0.8-113 (ED) 中的已知和已修复的问题

已知问题	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.0.8&sb=anfr&sts=open&srtBy=byRel&bt=custV
已修复的问题	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.0.8-113&sb=fr&svr=3nH&srtBy=byRel&bt=custV

其他漏洞搜索

步骤 1 转到 https://tools.cisco.com/bugsearch/。

步骤 2 使用思科帐户凭据登录。

步骤 3 输入搜索条件。

例如在“搜索”(Search for) 字段输入漏洞 ID 编号。

注意 用于之前 AsyncOS 版本 的 5 位漏洞编号不能在此工具中使用。

步骤 4 如果您有任何疑问或问题，请点击工具右上角的**帮助 (Help)** 或**反馈 (Feedback)** 链接。

相关文档

此产品的文档可从
http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html 获取。

思科内容安全管理设备的文档可从
http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html 获取。

支持

知识库

您可以通过以下 URL 访问思科客户支持网站上的思科知识库：

http://www.cisco.com/web/ironport/knowledgebase.html

注意 您需要 Cisco.com 用户 ID 才能访问网站。如果您没有 Cisco.com 用户 ID，您可以点击以下链接进行注册：`https://tools.cisco.com/RPF/register/register.do`

思科支持社区

思科支持社区是一个面向思科客户、合作伙伴和员工的在线论坛。它提供了一个场所，供相关人员讨论常规的网络安全问题以及有关思科具体产品的技术信息。您可以在论坛中发布主题，以咨询问题并与其他思科用户分享信息。

通过以下 URL 访问思科支持社区以了解网络安全和关联管理：

https://supportforums.cisco.com/community/5786/web-security

客户支持

国际：访问 http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

支持网站：访问 http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

对于普通问题，您还可以打开设备中的客户支持。如需相关指导，请参阅《用户指南》或联机帮助。

本文档需结合“相关文档”一节中列出的文档共同使用。