2017 年 11 月 13 日，星期一

漏洞聚焦：Foscam C1 室内高清摄像机存在多个漏洞

这些漏洞的发现者为思科 Talos 团队的 Claudio Bozzato。

执行摘要

Foscam C1 室内高清摄像机是一款基于网络的摄像机，可用于多种用途，包括用作家庭安全监控设备。最近，Talos 确定了这些设备中存在的几个漏洞，并与 Foscam 合作开发了修补程序。我们在一篇博客中发布了这些修补程序的详细信息，请点击此处阅读。在我们继续对这些设备进行安全评估时，Talos 又发现了其他漏洞。根据我们负责任的披露政策，Talos 已与 Foscam 展开合作，确保这些问题得以解决，并向受影响的客户提供固件更新。攻击者可以利用这些漏洞在受影响的设备上实现远程代码执行，并将欺诈性固件映像上传到设备，进而完全控制设备。

Foscam IP 视频摄像机网络服务 DDNS 客户端代码执行漏洞

Foscam C1 室内高清摄像机在启用了动态 DNS (DDNS) 的设备上易受几个缓冲区溢出漏洞的影响。在启用了 DDNS 的设备上，攻击者可以通过欺诈性 HTTP 服务器利用这些漏洞。当设备启动时，会派生一个线程，对已配置的 DDNS 服务器进行定期检查，查找与 DDNS 服务器相关的 IP 地址更新或更改。在将设备配置为使用 DDNS 的情况下，设备将向 DDNS 服务器发送请求并将关联的响应写入缓冲区，但不执行适当的边界检查。这可能会被攻击者控制的服务器利用，返回大于已分配缓冲区的特制响应而导致溢出，从而在受影响的设备上实现远程代码执行。下列公告和 CVE 都与此漏洞有关。

- Foscam IP 视频摄像机网络服务 oray.com DDNS 客户端代码执行漏洞 (TALOS-2017-0357 / CVE-2017-2854)
- Foscam IP 视频摄像机网络服务 3322.net DDNS 客户端代码执行漏洞 (TALOS-2017-0358 / CVE-2017-2855)
- Foscam IP 视频摄像机网络服务 dyndns.com DDNS 客户端代码执行漏洞 (TALOS-2017-0359 / CVE-2017-2856)
- Foscam IP 视频摄像机网络服务 9299.org DDNS 客户端代码执行漏洞 (TALOS-2017-0360 / CVE-2017-2857)

Foscam IP 视频摄像机 CGIProxy.fcgi 固件升级未签名映像漏洞 (TALOS-2017-0379 / CVE-2017-2872)

Foscam C1 室内高清摄像机允许通过设备上的 Web 管理界面执行固件升级。这些设备缺乏对用户提供的固件映像的充分安全验证。攻击者可以利用此功能和验证缺乏，向受影响的设备上传并执行自定义固件映像。为执行固件升级流程，攻击者可能需要访问在设备上具有管理员权限的帐户。我们已为 TALOS-2017-0379 分配漏洞代码 CVE-2017-2872。有关其他信息，请参阅此处的公告。

Foscam IP 视频摄像机 CGIProxy.fcgi SoftAP 配置命令注入漏洞 (TALOS-2017-0380/CVE-2017-2873)

Foscam C1 高清室内摄像机提供使用 Web 管理界面配置 SoftAP 的功能。SoftAP 配置有助于通过无线连接到设备，以执行初始设备设置和配置。这些设备易受“devMng”二进制文件中存在的命令注入漏洞的影响，该文件可通过“setSoftApConfig”命令访问。攻击者可以利用此漏洞来执行任意操作系统命令。要利用此漏洞，攻击者需要使用具有管理员权限的帐户访问受影响的设备。我们已为 TALOS-2017-0380 分配漏洞代码 CVE-2017-2873。有关其他信息，请参阅此处的公告。

Foscam IP 视频摄像机 devMng 多摄像头端口 10000 命令 0x0000 信息泄露漏洞 (TALOS-2017-0381/CVE-2017-2874)

Foscam C1 高清室内摄像机允许通过 UDP/10000 和 UDP/10001 进行设备到设备通信。这些通信旨在允许用户使用集中的 Web 管理界面，显示来自多个设备的视频流。这些设备易受信息泄漏漏洞的影响。未经身份验证的远程攻击者可以利用此漏洞获取敏感的设备信息，如 MAC 地址、摄像机名称和固件版本。我们已为 TALOS-2017-0381 分配漏洞代码 CVE-2017-2874。有关其他信息，请参阅此处的公告。

Foscam IP 视频摄像机 devMng 多摄像头端口 10000 命令 0x0002 用户名字段代码执行漏洞 (TALOS-2017-0382/CVE-2017-2875)

Foscam C1 高清室内摄像机允许通过 UDP/10000 和 UDP/10001 进行设备到设备通信。这些通信旨在允许用户使用集中的 Web 管理界面，显示来自多个设备的视频流。这些设备容易受到缓冲区溢出情况的影响，未经身份验证的远程攻击者可以利用该情况在受影响的设备上实施远程代码执行。该漏洞产生的原因是在身份验证请求期间，对提交的用户名参数的内容缺乏适当的边界检查。我们已为 TALOS-2017-0382 分配漏洞代码 CVE-2017-2875。有关其他信息，请参阅此处的公告。

Foscam IP 视频摄像机 devMng 多摄像头端口 10000 命令 0x0002 密码字段代码执行漏洞(TALOS-2017-0383/CVE-2017-2876)

Foscam C1 高清室内摄像机允许通过 UDP/10000 和 UDP/10001 进行设备到设备通信。这些通信旨在允许用户使用集中的 Web 管理界面，显示来自多个设备的视频流。这些设备容易受到缓冲区溢出情况的影响，未经身份验证的远程攻击者可以利用该情况在受影响的设备上实施远程代码执行。该漏洞产生的原因是在身份验证请求期间，对提交的密码参数的内容缺乏适当的边界检查。我们已为 TALOS-2017-0383 分配漏洞代码 CVE-2017-2876。有关其他信息，请参阅此处的公告。

Foscam IP 视频摄像机 devMng 多摄像头端口 10001 命令 0x0064 空漏洞 (TALOS-2017-0384/CVE-2017-2877)

Foscam C1 高清室内摄像机允许通过 UDP/10000 和 UDP/10001 进行设备到设备通信。这些通信旨在允许用户使用集中的 Web 管理界面，显示来自多个设备的视频流。这些设备易受一种情况的影响，即未经身份验证的攻击者可以通过 UDP/10001 向受影响的设备发送特制的网络数据包，从而将设备上配置的用户帐户重置为出厂默认设置。由于缺少错误检查，因此有可能无需在重置帐户的请求中指定有效的“authResetKey”值便可重置用户帐户。我们已为 TALOS-2017-0384 分配漏洞代码 CVE-2017-2877。有关其他信息，请参阅此处的公告。

Foscam IP 视频摄像机 CGIProxy.fcgi logOut 代码执行漏洞 (TALOS-2017-0385/CVE-2017-2878)

Foscam C1 高清室内摄像机易受缓冲区溢出情况的影响，而在 Web 管理界面执行“logOut”命令会出现此情况。攻击者可能会利用该漏洞在受影响的设备上实施远程代码执行。要利用此漏洞，攻击者需要通过设备的身份验证，即使是使用受限的“访客”账户。我们已为 TALOS-2017-0385 分配漏洞代码 CVE-2017-2878。有关其他信息，请参阅此处的公告。

Foscam IP 视频摄像机 UPnP 发现代码执行漏洞 (TALOS-2017-0386 / CVE-2017-2879)

Foscam C1 高清室内摄像机采用 UPnP 实现，旨在使设备能够与网络网关进行通信，以便远程访问设备的 Web 管理界面。Foscam C1 所使用的 UPnP 实现容易受到缓冲区溢出情况的影响，攻击者可以利用该情况在受影响的设备上进行远程代码执行。远程攻击者可以通过向受影响的设备发送特制的 UPnP 发现响应，来触发此漏洞。我们已为 TALOS-2017-0386 分配漏洞代码 CVE-2017-2879。有关其他信息，请参阅此处的公告。

测试的版本

经过测试，Talos 已确认以下 Foscam 固件版本受到感染：

Foscam 室内 IP 摄像头 C1 系列
系统固件版本：1.9.3.18
应用固件版本：2.52.2.43
插件版本：3.3.0.26

总结

Foscam C1 是部署最广泛的 IP 摄像头之一。很多情况下，这些设备可能部署在敏感位置。这些设备的市场用途为安全监控，许多人使用这些设备远程监控他们的住宅、孩子和宠物。因此，我们强烈建议这些设备上运行的固件保持最新，以确保设备的完整性，以及信息和所监控环境的机密性。Foscam 已发布固件更新，用来此处解决这些问题。受影响设备的用户应尽快更新到这一新版本，确保设备不容易受到攻击。

防护

以下 Snort 规则可以检测相关的漏洞攻击尝试活动。请注意，Talos 未来可能会发布更多规则，当前规则会根据未来得到的更多漏洞信息而有所变更。如需获取有关最新规则的信息，请参阅防御中心或 Snort.org。

Snort 规则：42432 - 42434、43080 - 43082、43555 - 43558、43713、43717。

发布者：EDMUND BRUMAGHIN；发布时间：10:43

标签：FOSCAM、IOT、漏洞、漏洞聚焦