解决由于多个CRL下载URL的CDP URL不匹配而导致的IOS XE证书验证故障

目录

问题

将附加CRL下载URL位置添加到动态多点VPN(DMVPN)中心设备后，由于IKE协商失败，某些分支隧道无法建立，并且中心记录了此错误：

```
%PKI-3-CERTIFICATE_INVALID: Certificate chain validation has failed
```

尽管证书链验证成功且成功下载CRL，但撤销检查会间歇性失败，原因如下：

```
No CRL found with matching CDP
revocation status = 2
```

当DMVPN中心路由器使用指向同一CRL文件的多个证书撤销列表(CRL)下载URL位置时，会出现此问题。CRL下载位置包括基于IP和基于FQDN的URL，而颁发给分支路由器的证书在其CRL分发点(CDP)中仅具有基于FQDN的URL。

环境

- 运行IOS® XE软件的Cisco设备，使用基于证书的IKE身份验证配置用于IPsec。
- 多个CRL下载位置，具有托管相同CRL文件的基于IP和基于FQDN的URL。
- 颁发给对等设备的证书的CDP中只有一个URL。
- IPsec隧道配置，在执行证书撤销检查时使用基于证书的身份验证。

分辨率

解决方案涉及在PKI环境中对单个规范CDP URL进行标准化，以确保CRL验证期间的URL精确匹配。

建议实施步骤

1.如果基于IP的CRL URL不是证书CDP的一部分，请从集线器配置中删除基于IP的CRL下载URL

```
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA1.crl
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA2.crl
```

2.仅配置与分支证书中的CDP匹配的基于FQDN的CRL下载URL

```
crypto pki crl download url http://crl.examplecompnay.com/prod/Example%20Company%20Issuing%20CA1.crl
crypto pki crl download url http://crl.examplecompany.com/prod/Example%20Company%20Issuing%20CA2.crl
```

3.更新发布CA模板以使用一致的CDP URL

确保颁发的CA模板仅将基于FQDN的CDP URL标记到新颁发的证书中。

4.重新注册中心辐射型证书（如果更改为新的CDP URL）

如果实施新的CDP URL，请更改发布CA以发布新的CDP URL，并重新注册中心证书和分支证书以承载新的URL。

冗余实施

例如，要使CRL提供程序冗余在不同的URL位置发布相同的CRL以防止托管设备发生故障，请使用以下方式在单个FQDN后实施后端冗余：

- DNS故障切换
- 负载均衡器
- 冗余CRL基础设施

请勿使用具有不同主机名/IP的多个CDP，因为IOS XE会将这些不同的CDP视为不同的CDP，即使它们引用相同的CRL文件也是如此。

确认

实施更改后，验证CRL缓存和隧道建立：

```
show crypto pki crl
```

确认IKEv2会话已成功建立：

```
show crypto session details
```

原因

此问题是由于CRL验证期间IOS XE精确CDP URL匹配行为引起的。当验证已启用撤销检查crl的对等证书时，IOS XE会在嵌入在要验证的证书中的CDP URL与存储在集线器的解析CRL缓存中的CRL关联的CDP URL之间执行精确字符串匹配。

出现以下故障序列：

1. 集线器使用基于IP的CDP URL成功下载CRL，并在该URL下将其内部缓存。
2. 分支证书在其CDP中引用基于FQDN的URL。
3. 在吊销验证期间，IOS XE会搜索与FQDN URL匹配的缓存CRL。
4. 由于IOS XE将基于IP的URL和基于FQDN的URL视为不同的CDP，因此找不到完全匹配。
5. 路由器返回“No CRL found with matching CDP”（未找到具有匹配CDP的CRL），且撤销状态 = 2。
6. 证书验证失败，出现%PKI-3-CERTIFICATE_INVALID。

IOS XE不会将不同的URL格式（IP与FQDN）规范化为等效格式，即使两个格式都返回同一颁发者的相同CRL内容时也是如此。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。