VSRC 安全周报（2021-09-27）

0x00 本周漏洞综述

本周需要关注漏洞共 3 个：Netgear Circle 远程代码执行漏洞（CVE-2021-40847）；VMware vCenter Server 文件上传漏洞（CVE-2021-22005）；SonicWall SMA 100 系列任意文件删除漏洞（CVE-2021-20034）。

本周安全态势共 1 个：CVE-2021-38112：AWS WorkSpaces RCE 漏洞分析。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Netgear Circle 远程代码执行漏洞（CVE-2021-40847）

漏洞概况

CVE ID	CVE-2021-40847	时 间	2021-09-20
类 型	RCE	等 级	高危
远程利用	是	影响范围	
攻击复杂度	高	可用性	高
用户交互	无	所需权限	无
PoC/EXP	已公开	在野利用	

漏洞详情

2021 年 9 月 20 日，Netgear 发布安全公告，修复了在 Circle parental control service

（Circle 家长控制服务）中发现的一个远程代码执行漏洞（CVE-2021-40847），该漏洞的 CVSSv3 评分为 8.1。

Circle 家长控制服务在多种 Netgear 小型办公室/家庭办公室 (SOHO) 设备上以 root 权限运行。由于 Netgear 路由器上的 Circle 家长控制服务存在不安全的更新过程，具有网络访问权限的远程攻击者可以通过中间人（MitM）攻击以 root 权限远程执行代码。

虽然家长控制本身在路由器上默认没有启用，但 Circle 的更新守护进程默认是启用的。该守护程序连接到 Circle 和 NETGEAR，以获得版本信息和 circled 守护程序及其过滤数据库的更新。然而，NETGEAR 的数据库更新是没有签名的，并通过明文 HTTP 下载。因此，能够对设备进行 MitM 攻击的攻击者可以用恶意制作的压缩数据库文件响应 circled 更新请求，提取该文件后，攻击者可以用控制的代码覆盖可执行文件。之后，攻击者可以完全控制通过受感染路由器的网络流量，从而读取与其它设备交换的加密数据，甚至可以通过攻击链破坏 ISP 或企业网络。

影响范围

易受攻击的 Netgear 路由器	补丁版本
R6400v2	固件版本 1.0.4.120
R6700	固件版本 1.0.2.26
R6700v3	固件版本 1.0.4.120
R6900	固件版本 1.0.2.26
R6900P	固件版本 3.3.142_HOTFIX
R7000	固件版本 1.0.11.128
R7000	固件版本 1.3.3.142_HOTFIX
R7850	固件版本 1.0.5.76
R7900	固件版本 1.0.4.46
R8000	固件版本 1.0.4.76
RS400	固件版本 1.5.1.80

安全建议

目前该漏洞已经修复，建议受影响的用户及时升级更新。

NETGEAR 产品下载最新固件：

1.访问 NETGEAR 支持。

2.在搜索框中输入您的型号，然后在下拉菜单中选择您的型号。

如果您没有看到下拉菜单，请确保您输入了正确的型号，或者选择一个产品类别来浏览您的产品型号。

3.单击下载。

4.在当前版本下，选择标题以固件版本开头的第一个下载。

5.单击发行说明。

6.按照固件发行说明中的说明下载并安装新固件。

下载链接：

https://www.netgear.com/support/

参考链接：

https://kb.netgear.com/000064039/Security-Advisory-for-Remote-Code-Execution-on-Some-Routers-PSV-2021-0204

https://blog.grimm-co.com/2021/09/mama-always-told-me-not-to-trust.html

https://www.bleepingcomputer.com/news/security/netgear-fixes-dangerous-code-execution-bug-in-multiple-routers/

2. VMware vCenter Server 文件上传漏洞（CVE-2021-22005）

漏洞概况

CVE ID	CVE-2021-22005	时 间	2021-09-21
类 型	文件上传	等 级	严重
远程利用	是	影响范围	
攻击复杂度	低	可用性	高
用户交互	无	所需权限	无
PoC/EXP	未公开	在野利用	

漏洞详情

2021 年 9 月 21 日，VMware 发布安全公告，公开披露了 vCenter Server 中的 19 个安全漏洞，这些漏洞的 CVSSv3 评分范围为 4.3-9.8。

其中，最为严重的漏洞为 vCenter Server 中的任意文件上传漏洞(CVE-2021-22005)，该漏洞存在于 vCenter Server 的分析服务中，其 CVSSv3 评分为 9.8。能够网络访问 vCenter Server 上的 443 端口的攻击者可以通过上传恶意文件在 vCenter Server 上远程执行代码。该漏洞无需经过身份验证即可远程利用，攻击复杂度低，且无需用户交互。

根据 Shodan 的搜索结果，数以千计的 vCenter Server 可通过互联网访问并受到攻击 。目前已经检测到攻击者正在扫描和攻击存在漏洞的 VMware vCenter 服务器。

除 CVE-2021-22005 之外，VMware 还修复了 vCenter Server 中的其它 18 个安全漏洞：

- CVE-2021-21991：vCenter Server 本地提权漏洞（CVSSv3 评分 8.8）

- CVE-2021-22006：vCenter Server 反向代理绕过漏洞（CVSSv3 评分 8.3）
- CVE-2021-22011：vCenter Server 未经身份验证的 API 端点漏洞（CVSSv3 评分 8.1）
- CVE-2021-22015：vCenter Server 本地提权漏洞（CVSSv3 评分 7.8）
- CVE-2021-22012：vCenter Server 未经身份验证的 API 信息泄露漏洞（CVSSv3 评分 7.5）
- CVE-2021-22013：vCenter Server 路径遍历漏洞（CVSSv3 评分 7.5）
- CVE-2021-22016：vCenter Server 反射型 XSS 漏洞（CVSSv3 评分 7.5）
- CVE-2021-22017：vCenter Server rhttpproxy 绕过漏洞（CVSSv3 评分 7.3）
- CVE-2021-22014：vCenter Server 身份验证代码执行漏洞（CVSSv3 评分 7.2）
- CVE-2021-22018：vCenter Server 文件删除漏洞（CVSSv3 评分 6.5）
- CVE-2021-21992：vCenter Server XML 解析拒绝服务漏洞（CVSSv3 评分 6.5）
- CVE-2021-22007：vCenter Server 本地信息泄露漏洞（CVSSv3 评分 5.5）
- CVE-2021-22019：vCenter Server 拒绝服务漏洞（CVSSv3 评分 5.3）
- CVE-2021-22009：vCenter Server VAPI 拒绝服务漏洞（CVSSv3 评分 5.3）
- CVE-2021-22010：vCenter Server VPXD 拒绝服务漏洞（CVSSv3 评分 5.3）
- CVE-2021-22008：vCenter Server 信息泄露漏洞（CVSSv3 评分 5.3）
- CVE-2021-22020：vCenter Server Analytics 服务拒绝服务漏洞（CVSSv3 评分 5.0）
- CVE-2021-21993：vCenter Server SSRF 漏洞（CVSSv3 评分 4.3）

影响范围

CVE-2021-22005：

VMware vCenter Server 7.0

VMware vCenter Server 6.7

注：CVE-2021-22005 会影响所有默认配置的 vCenter Server 6.7 和 7.0 部署，不会影响 vCenter Server 6.5。其它 18 个漏洞的影响范围请参见 VMware 官方公告。

安全建议

目前 VMware 已经发布了相关漏洞的补丁，建议受影响的用户参考 VMware 官方公告及时升级更新。

下载链接：

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

https://www.bleepingcomputer.com/news/security/hackers-are-scanning-for-vmware-cve-2021-22005-targets-patch-now/

https://threatpost.com/vmware-ransomware-bug-vcenter-server/174901/

3. SonicWall SMA 100 系列任意文件删除漏洞（CVE-2021-20034）

漏洞概况

CVE ID	CVE-2021-20034	时 间	2021-09-23
类 型	文件删除	等 级	严重
远程利用	是	影响范围	
攻击复杂度	低	可用性	高
用户交互	无	所需权限	无
PoC/EXP	未公开	在野利用	否

漏洞详情

2021 年 9 月 24 日，SonicWall 发布安全公告，修复了 SMA 100 系列设备（包括 SMA 200、210、400、410 和 500v）中的一个任意文件删除漏洞（CVE-2021-20034），该漏洞的 CVSSv3 评分为 9.1。

由于对文件路径限制不当，未经身份验证的远程攻击者可以绕过路径遍历检查并从 SMA 100 系列设备上删除任意文件，最终攻击者能够获得对该设备的管理员权限，或导致设备重新启动到出厂默认设置。

影响范围

产品	平台	受影响版本	修复版本
	• SMA 200 • SMA 210	10.2.1.0-17sv 及之前版本	10.2.1.1-19sv 或更高版本

SMA 100 系列	• SMA 400 • SMA 410 • SMA 500v（ESX、KVM、AWS、Azure）		
		10.2.0.7-34sv 及之前版本	10.2.0.8-37sv 或更高版本
		9.0.0.10-28sv 及之前版本	9.0.0.11 -31sv 或更高版本

安全建议

目前该漏洞已经修复，建议受影响的用户及时升级更新到修复版本。

下载链接：

https://mysonicwall.com/

参考链接：

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0021

https://www.sonicwall.com/support/product-notification/security-notice-critical-arbitrary-file-delete-vulnerability-in-sonicwall-sma-100-series-appliances/210819124854603/

https://www.bleepingcomputer.com/news/security/sonicwall-fixes-critical-bug-allowing-sma-100-device-takeover/

0x02 本周安全态势

1. CVE-2021-38112：AWS WorkSpaces RCE 漏洞分析

概述

本文详细介绍了 Rhino 安全实验室在 AWS WorkSpaces 桌面客户端中发现的一个漏洞，追踪为CVE-2021-38112，如果受害者从他们的浏览器中打开恶意的WorkSpaces URI，则可以利用该漏洞远程执行命令。Rhino 向 Amazon 报告了该漏洞，并立即对其进行了修复。3.1.9 之前的 AWS WorkSpaces 桌面客户端版本受该漏洞影响。

利用此 AWS WorkSpaces 漏洞能够在已安装 WorkSpace 客户端的系统上远程执行代码。该漏洞还允许攻击者在 WorkSpaces 客户端中配置代理设置，或在受害者合法访问其 WorkSpaces 环境时键盘记录用户名和密码，从而进入 AWS WorkSpaces 主机。

Amazon WorkSpaces

Amazon WorkSpaces 是一项完全托管的持久桌面虚拟化服务，使用户能够随时随地从任何受支持的设备上访问他们需要的数据、应用程序和资源。可以使用 Amazon WorkSpaces 在短短几分钟内配置 Windows 或 Linux 桌面，并迅速扩大规模以向全球各地的员工提供成千上万的桌面。Amazon WorkSpaces 部署在亚马逊虚拟私有云（VPC）内，用户数据不会存储在本地设备上。这有助于提高用户数据的安全性并降低整体风险。

访问 Amazon WorkSpaces 的方式有很多，其中一种是使用桌面客户端，它能够直接连接到 WorkSpace。桌面客户端可以方便地注册自定义 URI，用户只需单击浏览器中的链接即可快速启动到 WorkSpace。

AWS RCE 漏洞细节

当 WorkSpaces 桌面客户端安装在 Windows 计算机上时，它会向系统注册一个自

定义 URI (workspaces://)。这允许通过在浏览器中访问自定义 URI 来启动 WorkSpaces。在处理 URI 的过程中，WorkSpaces 应用程序未能对参数进行清理，这些参数随后在向 WorkSpace 进行身份验证时被传递到命令行。由于 WorkSpaces 客户端基于 Chromium 嵌入式框架（CEF），这允许将参数注入到命令行中，滥用已知的调试 CEF 命令行参数（-gpu-launcher），最终导致任意命令被执行。

当通过自定义 URI 启动应用程序时，浏览器会将 URI 作为第一个参数传递给命令行上的应用程序，然后应用程序可以根据需要处理 URI。在浏览器中，通过在 URI 中对特殊字符进行 URL 编码，在应用程序初始启动时阻止命令和参数注入，防止诸如双引号或其他命令行控制字符之类的东西被注入以脱离预期的命令。当 WorkSpaces URL 解码并使用 URI 参数中的参数来启动新命令而不清理参数时，Amazon WorkSpaces 就会出现安全问题，可以注入任意参数。

UriSchemeGateway

```
35              StartUpConfigDto startUpConfigDto = this.ParseHostAndQuery(uriString);
36              return this._interactor.ProcessStartUpConfigDto(startUpConfigDto);
37          }
38
39          // Token: 0x060005EB RID: 1515 RVA: 0x00004EAB File Offset: 0x000030AB
40          public bool ShouldNotInterruptCurrentSession()
41          {
42              return this._interactor.ShouldNotInterruptCurrentSession();
43          }
44
45          // Token: 0x060005EC RID: 1516 RVA: 0x0001CEF0 File Offset: 0x0001B0F0
46          private StartUpConfigDto ParseHostAndQuery(string uriString)
47          {
48              StartUpConfigDto startUpConfigDto = new StartUpConfigDto();
49              if (uriString.Contains("@"))
50              {
51                  string[] array = uriString.Split('@', StringSplitOptions.None);
52                  startUpConfigDto.Username = Uri.UnescapeDataString(array[0]);
53                  if (array.Length != 2)
54                  {
55                      return null;
56                  }
57                  uriString = array[1];
58              }
59              string[] array2 = uriString.Split('?', StringSplitOptions.None);
60              string text = array2[0];
61              if (!string.IsNullOrWhiteSpace(text) && text[text.Length - 1] == '/')
62              {
63                  text = text.Remove(text.Length - 1);
64              }
65              if (string.IsNullOrWhiteSpace(text))
66              {
67                  return null;
68              }
69              startUpConfigDto.RegCode = Uri.UnescapeDataString(text);
70              if (array2.Length == 2)
```

来自反编译的 WorkSpacesClient.Common.dll 的 UriSchemeGateway 类，它处理自定

义 URI

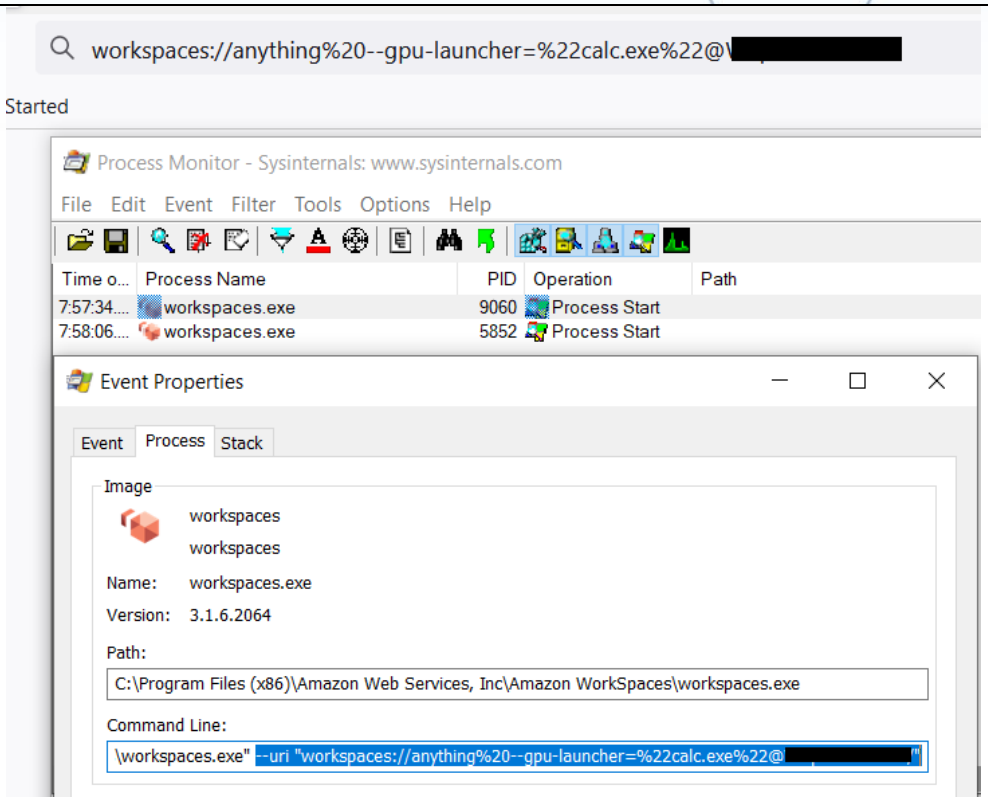
可以看到从 URI 字符串中解析出 username、RegCode 和 host 等各种参数。然后使用 Uri.UnescapeDataString 方法对每个参数进行 URL 解码，然后将其添加到 startUpConfigDto 对象中。之后，startUpConfigDto 对象被传递给 ProcessStartUpConfigDto 以启动该进程。

这里唯一的问题是在启动过程中验证 RegCode 参数以确保它是有效的 WorkSpaces 注册码。但是任何拥有 AWS 账户的人都可以使用他们自己的有效 WorkSpaces 注册码来满足这一要求。为此，只需配置一个 AWS Managed Active Directory 用户，并为该用户设置一个 WorkSpace。

生成一个 URI 来执行命令现在变得非常简单。在 AWS 账户中设置 AWS WorkSpaces 并为用户获取有效的注册码。注入"-gpu-launcher"参数，指定一个 CEF 将执行的任意命令。

```
workspaces://anything%20--gpu-launcher=%22calc.exe%22@REGISTRATION_CODE
```

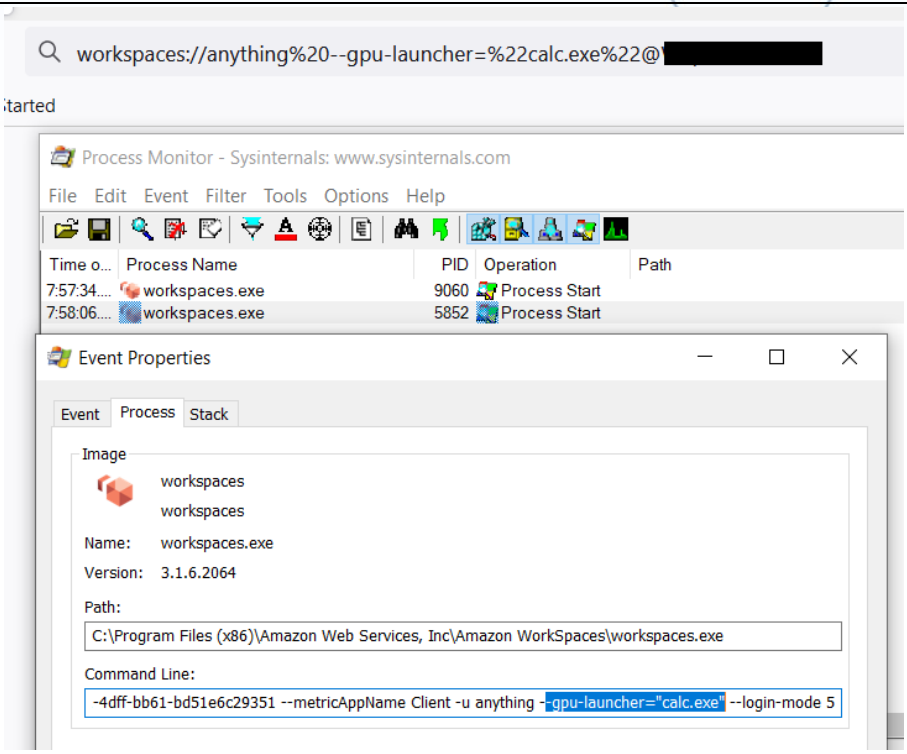
可以在 Process Monitor 中看到有两个 workspaces.exe 的执行情况。第一个是从浏览器初始启动，命令行和预期的一样，是 URL 编码的。



在 Process Monitor 中首次启动 WorkSpaces

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces\workspaces.exe" --uri "workspaces://anything%20--gpu-launcher=%22calc.exe%22@REGISTRATION_CODE"
```

然后，workspaces.exe 进程会使用其他参数启动，包括我们注入的已被 URL 解码的参数。



在 Process Monitor 中二次启动 WorkSpaces

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces\workspaces.exe" --ws-pipe-name UUID --ws-pipe-handle 4576 -r REGISTRATION_CODE --auth-url https://<appssite>.awsapps.com:443/login/?client_id=<clientid>&redirect_uri=https%3a%2f%2fskylight.local&locale=en_US --org-name <org name> --session-id <session id> --metricAppName Client -u anything --gpu-launcher="calc.exe" --login-mode 5
```

我们提供了 AWS WorkSpaces RCE 的 PoC，显示了在浏览器中打开一个精心制作的页面时的所有情况。虽然在默认情况下，用户需要允许 WorkSpaces 应用程序从浏览器中打开，但如果用户以前曾接受过这个提示，总是允许这样做，这将不需要用户交互。

结论

AWS 已在 3.1.9 固定版本中修复了此漏洞（2021 年 6 月 29 日发布），建议相关受影响用户及时升级更新。

此外，自定义 URI 可能很有用，对用户来说很方便，可以使他们更容易开始使用一些应用程序。尽管浏览器在确保自定义 URI 在传递到命令行之前被编码，以帮助防止参数和命令注入，但重要的是要考虑这些值在应用程序流程的其余部分是如何处理的。在使用 URI 参数或值的过程中需保持谨慎，因为输入仍然是不可信任的。

通用安全建议

- 定期更新软件、程序和应用程序，确保应用程序是最新的，以保护系统免受漏洞利用。
- 加强系统和网络的访问控制，修改防火墙策略，关闭非必要的应用端口或服务，减少将危险服务（如 SSH、RDP 等）暴露到公网，以减少攻击面。
- 加强系统用户和权限管理，启用多因素认证机制和最小权限原则，用户和软件权限应保持在最低限度；启用强密码策略并设置为定期修改。
- 预防 0day 漏洞和恶意软件，安全产品实时更新最新规则或相关防护指标。
- 使用最新、全面的威胁情报信息，监控网络和安全事件，以快速响应攻击。

原文链接：

https://rhinosecuritylabs.com/aws/cve-2021-38112-aws-workspaces-rce/?__cf_chl_jschl_tk__=pmd_XcEFdL6Sp_PtLOYR.E6GQyPehV7m3LXviDvdyKbv.qI-1632281490-0-gqNtZGzNAfujcnBszQhR