

```
it overrides the internal black and white lists that are hard-coded in this release.

Fling Note: until further notice all plugins are disabled by the HTML5 client except SDK samples.
Use this file to re-enable specific HTML plugins during your testing.
-->
<Matrix>
  <pluginsCompatibility>
    <!--
      WHITE LIST:
      Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
      <PluginPackage id="com.acme.myplugin" status="compatible"/>
      Or this to specify all versions greater or equal to 2.1.0:
      <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
      Or this to enable all plugins starting with com.acme:
      <PluginPackage id="com.acme.*" status="compatible"/>
    -->
    <PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
  </pluginsCompatibility>
-->
</Matrix>
-->
Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin.
<PluginPackage id="com.acme.myplugin" status="incompatible"/>
```

CVE-2021-21972 vCenter 6.5-7.0 RCE 漏洞分析

2021-02-24 17:59:59 Author: noahnblog.360.cn(查看原文) 阅读量:4937 收藏

0x01. 漏洞简介

vSphere 是 VMware 推出的虚拟化平台套件，包含 ESXi、vCenter Server 等一系列的软件。其中 vCenter Server 为 ESXi 的控制中心，可从单一控制点统一管理数据中心的所有 vSphere 主机和虚拟机，使得 IT 管理员能够提高控制能力，简化入场任务，并降低 IT 环境的管理复杂性与成本。

vSphere Client (HTML5) 在 vCenter Server 插件中存在一个远程执行代码漏洞。未授权的攻击者可以通过开放 443 端口的服务器向 vCenter Server 发送精心构造的请求，从而在服务器上写入 webshell，最终造成远程任意代码执行。

0x02. 影响范围

- vmware:vcenter_server 7.0 U1c 之前的 7.0 版本
- vmware:vcenter_server 6.7 U3l 之前的 6.7 版本
- vmware:vcenter_server 6.5 U3n 之前的 6.5 版本

0x03. 漏洞影响

VMware已评估此问题的严重程度为 **严重** 程度，CVSSv3 得分为 **9.8**。

0x04. 漏洞分析

vCenter Server 的 vROPS 插件的 API 未经过鉴权，存在一些敏感借口。其中 **uploadova** 接口存在一个上传 OVA 文件的功能：

```
@RequestMapping(
    value = {"/uploadova"},
    method = {RequestMethod.POST}
)
public void uploadOvaFile(@RequestParam(value = "uploadFile",required = true)
    logger.info("Entering uploadOvaFile api");
    int code = uploadFile.isEmpty() ? 400 : 200;
    PrintWriter wr = null;
    ...

    response.setStatus(code);
    String returnStatus = "SUCCESS";
    if (!uploadFile.isEmpty()) {
        try {
            logger.info("Downloading OVA file has been started");
            logger.info("Size of the file received  : " + uploadFile.getSize());
            InputStream inputStream = uploadFile.getInputStream();
            File dir = new File("/tmp/unicorn_ova_dir");
            if (!dir.exists()) {
                dir.mkdirs();
            } else {
                String[] entries = dir.list();
                String[] var9 = entries;
```

```
        File currentFile = new File(dir.getPath(), entry);
        currentFile.delete();
    }

    logger.info("Successfully cleaned : /tmp/unicorn_ova_dir");
}

TarArchiveInputStream in = new TarArchiveInputStream(inputStream);
TarArchiveEntry entry = in.getNextTarEntry();
ArrayList result = new ArrayList();
```

代码逻辑是将 TAR 文件解压后上传到 `/tmp/unicorn_ova_dir` 目录。注意到如下代码：

```
while(entry != null) {
    if (entry.isDirectory()) {
        entry = in.getNextTarEntry();
    } else {
        File curfile = new File("/tmp/unicorn_ova_dir", entry.getName());
        File parent = curfile.getParentFile();
        if (!parent.exists()) {
            parent.mkdirs();
        }
    }
}
```

直接将 TAR 的文件名与 `/tmp/unicorn_ova_dir` 拼接并写入文件。如果文件名内存在 `../` 即可实现目录遍历。

对于 Linux 版本，可以创建一个包含 `../../home/vsphere-ui/.ssh/authorized_keys` 的 TAR 文件并上传后利用 SSH 登陆：

```
$ ssh 192.168.1.34 -lvsphere-ui

VMware vCenter Server 7.0.1.00100

Type: vCenter Server with an embedded Platform Services Controller

vsphere-ui@bogon [ ~ ]$ id
uid=1016(vsphere-ui) gid=100(users) groups=100(users),59001(cis)
```

针对 Windows 版本，可以在目标服务器上写入 JSP webshell 文件，由于服务是 System 权限，所以可以任意文件写。

0x05. 漏洞修复

升级到安全版本：

- vCenter Server 7.0 版本升级到 7.0.U1c
- vCenter Server 6.7版本升级到 6.7.U3l
- vCenter Server 6.5版本升级到 6.5 U3n

临时修复建议

(针对暂时无法升级的服务器)

- SSH远连到vCSA（或远程桌面连接到Windows VC)
- 备份以下文件：
 - Linux系统文件路径为：`/etc/vmware/vsphere-ui/compatibility-matrix.xml` (vCSA)
 - Windows文件路径为：`C:\ProgramData\VMware\VCServer\cfg\vsphere-ui` (Windows VC)
- 使用文本编辑器将文件内容修改为：

```
<Matrix>
  <pluginsCompatibility>
    <!--
      WHITE LIST:
      Add this to enable all plugins whose plugin-package id is com.acme.example.myplugin:
      <PluginPackage id="com.acme.myplugin" status="compatible"/>
      Or this to specify all versions greater or equal to 2.1.0:
      <PluginPackage id="com.acme.myplugin" version=[2.1.0,] status="compatible"/>
      Or this to enable all plugins starting with com.acme:
      <PluginPackage id="com.acme.*" status="compatible"/>
    -->
    <PluginPackage id="com.vmware.vrops.install" status="incompatible"/>
  <!--
    BLACK LIST:
    Add this to disable a plugin whose plugin-package id is com.acme.example.myplugin:
    <PluginPackage id="com.acme.myplugin" status="incompatible"/>
  -->
</pluginsCompatibility>
</Matrix>
```

4. 使用vmon-cli -r vsphere-ui命令重启vsphere-ui服务
5. 访问https:///ui/vropspluginui/rest/services/checkmobregister，显示404错误



6. 在vSphere Client的Solutions->Client Plugins中VMWare vROPS插件显示为incompatible

vm vSphere Client

Menu

Search in all environments

Refresh

Help

Administrator@VSPHERE.LOCAL

Administration

Access Control

Roles

Global Permissions

Licensing

Licenses

Solutions

Client Plugins

vCenter Server Extensions

Deployment

System Configuration











Customer Experience Improvement P...

Support

Client Plugins

ENABLE

DISABLE

	Name	Version	Status	VMware Certified	Vendor	Description
<input type="radio"/>	 VMware Cloud Director Availability	0.4.0.0	 Deployed / Enabled	No	VMware	VMware Cloud Director Availability
<input type="radio"/>	 vCenter Server Life-cycle Manager	1.0.0.0	 Deployed / Enabled	No	VMware, Inc.	Life-cycle Management for vCenter Server
<input type="radio"/>	 VMware vSAN H5 Client Plugin	7.0.1.0	 Deployed / Enabled	No	VMware, Inc.	VMware vSAN H5 Client Plugin
<input type="radio"/>	 VMware vSphere Lifecycle Manager	7.0.116858590	 Deployed / Enabled	Yes	VMware	VMware vSphere Lifecycle Manager
<input type="radio"/>	 VMware vRops Client Plugin	7.0.1.0	 Incompatible	Unknown	VMware, Inc.	VMware vRops Client Plugin

0x06. 参考链接

VMware官方安全通告
https://www.vmware.com/security/advisories/VMSA-2021-0002.html
360Cert漏洞预警通告
https://mp.weixin.qq.com/s/7x5nBpHIVOI5c1kqfsIhSQ
官方漏洞缓释措施
https://kb.vmware.com/s/article/82374

文章来源: http://noahblog.360.cn/vcenter-6-5-7-0-rce-lou-dong-fen-xi/
如有侵权请联系:admin#unsafe.sh

0 Comments - powered by utteranc.es

Write

Preview

Sign in to comment

