بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

آسیب پذیری بحرانی WMware vCenter Server

خبر آسیب‌پذیری

شناسه سند	MaherReport_13991209-01
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۳۹۹/۱۲/۰۹
طبقه‌بندی سند	**عادی**

تهران، خیابان شهید بهشتی، نرسیده به قائم مقام فراهانی، پلاک ۲۶۷، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰

(۰۲۱) ۴۲۶۵۰۰۰۰

cert.ir

فهرست مطالب

۱ مقدمه ای بر آسیب‌پذیری‌ها ۱

۱-۱ آسیب پذیری vCenter Server با شناسه CVE-2021-21972 ..... ۱

۱-۱-۱ بررسی آسیب پذیر بودن یک vCenter Server به شناسه CVE-2021-21972 ..... ۱

۱-۲ آسیب پذیری vCenter Server با شناسه CVE-2021-21973 ..... ۲

۱-۳ آسیب پذیری ESXi با شناسه CVE-2021-21974 ..... ۲

۲ راه حل و توصیه های امنیتی ۲

۱ مقدمه ای بر آسیب‌پذیری‌ها

به تازگی دو آسیب‌پذیری در vCenter Server که نرم افزار مدیریتی سیستم‌های VMware vSphere می‌باشد و همچنین یک آسیب‌پذیری دیگر در VMWare ESXi شناسایی و مطابق جدول شماره ۱ آدرس‌دهی شده است.

جدول 1 : لیست آسیب پذیری های جدید WMware

CVE	Affected Product	CVSSv3	Type
CVE-2021-21972	vCenter Server	9.8	RCE
CVE-2021-21973	vCenter Server	5.3	SSRF
CVE-2021-21974	ESXi	8.8	Heap Overflow

۱-۱ آسیب پذیری vCenter Server با شناسه CVE-2021-21972

این آسیب پذیری اگرچه از عدم احراز هویت در پلاگین vRealize Operations vCenter ناشی می شود، اما در تمامی برنامه‌های vCenter Server که طبق پروسه‌ی پیش‌فرض نصب و پیکربندی شده باشند، فعال می‌باشد. بر این اساس مهاجم بدون احراز هویت و در اختیار داشتن دسترسی های لازم(unauthorized)، می‌تواند نسبت به اجرای کد از راه دور بر روی میزبان که از طریق پورت ۴۴۳ در دسترس می باشد اقدام و از این آسیب پذیری بهره برداری و سوءاستفاده کند.

۱-۱-۱ بررسی آسیب پذیر بودن یک vCenter Server به شناسه CVE-2021-21972

به منظور بررسی آسیب پذیر بودن یک vCenter Server ، می توان آدرس IP میزبان را در قالب زیر توسط مرورگر فراخوانی کرد:

```
https://<VC-IP-or-FQDN>/ui/vropspluginui/rest/services/uploadova
```

درصورت مشاهده پیغام خطای ۴۰۵ مطابق تصویر ۱، آسیب پذیر بودن برنامه به شناسه CVE-2021-21972 محرز می‌شود.

تصویر ۱ : بررسی آسیب پذیر بودن یک vCenter Server به شناسه CVE-2021-21972

۱-۲ آسیب پذیری vCenter Server با شناسه CVE-2021-21973

برنامه vSphere Client (HTML5) به جهت اعتبارسنجی نادرست آدرس های URL در پلاگین vCenter Server دارای یک ضعف امنیتی جعل درخواست سمت سرور یا SSRF می باشد. بر این اساس مهاجم با دسترسی تحت شبکه به پورت ۴۴۳ می تواند با ارسال درخواست POST به پلاگین vCenter Server از این ضعف بهره برداری کرده و منجر به افشای اطلاعات شود.

وجود این ضعف امنیتی در نسخه های 7.X (نسخه های پیش از 7.0 U1c)، نسخه های 6.7 (نسخه های پیش از 6.7 U3I) و نسخه های 6.5 (نسخه های پیش از 6.5 U3n) از WMware vCenter Server و همچنین نسخه های 4.X (نسخه های پیش از 4.2) و نسخه های 3.X (نسخه های پیش از 3.10.1.2) از WMware Cloud Foundation تایید شده است. vCenter Server با شناسه CVE-2021-21973

۱-۳ آسیب پذیری ESXi با شناسه CVE-2021-21974

یک ضعف امنیتی از نوع سرریز پشته یا Heap-OverFlow در سرویس OpenSLP مورد استفاده در WMware ESXi شناسایی شده است. بر این اساس مهاجمی که در شبکه ای مشترک با ESXi بوده و به پورت ۴۲۷ نیز دسترسی داشته باشد، قادر خواهد بود از ضعف سرریز پشته سوءاستفاده کرده و موفق به اجرای کد از راه دور گردد.

۲ راه حل و توصیه های امنیتی

مطابق توصیه نامه منتشر شده توسط VMware، نسخه های تحت تاثیر این آسیب پذیری ها، صرف نظر از سیستم عاملی که آن ها را میزبانی می کنند، می بایست متناسب با جدول شماره ۲ در اسرع وقت به روزرسانی شوند.

جدول2 : نسخه های آسیب پذیر به شناسه های CVE-2021-2197X و نسخه های وصله شده ی آن

محصول	شناسه CVE	CVSSv3	نسخه آسیب پذیر	نسخه وصل شده
vCenter Server	CVE-2021-21972	9.8	7.0	7.0 U1c
		9.8	6.7	6.7 U3l
		9.8	6.5	6.5 U3n
	CVE-2021-21973	5.3	7.0	7.0 U1c
		5.3	6.7	6.7 U3l
		5.3	6.5	6.5 U3n
Cloud Foundation (vCenter Server)	CVE-2021-21972	9.8	4.X	4.2
		9.8	3.X	3.10.1.2
	CVE-2021-21973	5.3	4.X	4.2
		5.3	3.X	3.10.1.2
ESXi	CVE-2021-21974	8.8	7.0	ESXi70U1c-17325551
		8.8	6.7	ESXi670-202102401-SG
		8.8	6.5	ESXi650-202102101-SG
Cloud Foundation (ESXi)		8.8	4.X	4.2
		8.8	3.X	روش وصله موقت در آدرس https://kb.vmware.com/s/article/82705

چنانچه در حال حاضر امکان بروزرسانی برنامه ها امکان پذیر نیست، می توان به صورت موقت دسترسی به پورت ۴۴۳ (در موارد آسیب پذیر به CVE-2021-21972/3) و یا پورت ۴۲۷ (در موارد آسیب پذیر به CVE-2021-21974) را محدود کرد. همچنین مطابق با توصیه نامه Vmware می‌توان/می بایست درخصوص آسیب‌پذیری های CVE-2021-21972/3، متناسب با سیستم عامل میزبان و به صورت موقت تا زمان انجام بروزرسانی کامل، اقداماتی به شرح ذیل اتخاذ شود:

۱- به میزبان متصل شوید:

- در میزبان مجازی مبتنی بر لینوکس (vCSA):
  - از طریق SSH به vCSA متصل شوید.
- در میزبان مجازی مبتنی بر ویندوز:
  - با استفاده از مکانیزم RDP به vCenter Server مبتنی بر ویندوز متصل شوید.

۲- یک نسخه پشتیبان از فایل compatibility-matrix.xml که محتویاتی مطابق تصویر شماره ۲ دارد، تهیه نمایید.

```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    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"/>
        -->

        <!--
            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>
```

تصویر ۲ : محتوای فایل compatibility-matrix.xml

- در میزبان مجازی مبتنی بر لینوکس (vCSA) این فایل در آدرس زیر قرار دارد:

```
/etc/vmware/vsphere-ui/compatibility-matrix.xml
```

- در میزبان مجازی مبتنی بر ویندوز این فایل در آدرس زیر قرار دارد:

```
C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\compatibility-matrix.xml
```

۳- خط زیر را به کمک یک ویرایشگر، مطابق تصویر شماره ۳ در میان تگ pluginsCompatibility قرار داده و فایل را ذخیره نمایید.

```
<!--
    This file lets you define a WHITE LIST and a BLACK LIST of plugins to control your own setup.
    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"/>
        <!--
            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>
```

تصویر ۳ : محتوای فایل compatibility-matrix.xml پس از ویرایش

۴- با توجه به سیستم عامل میزبان، نسبت به راه اندازی مجدد سرویس vsphere-ui اقدام نمایید:

- با استفاده از خط دستوری زیر در میزبان مجازی مبتنی بر لینوکس (vCSA):

```
service-control --restart vsphere-ui
```

- با استفاده از خط دستوری زیر در کنسول cmd میزبان مجازی مبتنی بر ویندوز:

```
C:\Program Files\VMware\vCenter Server\bin> service-control --
restart vsphere-ui
```

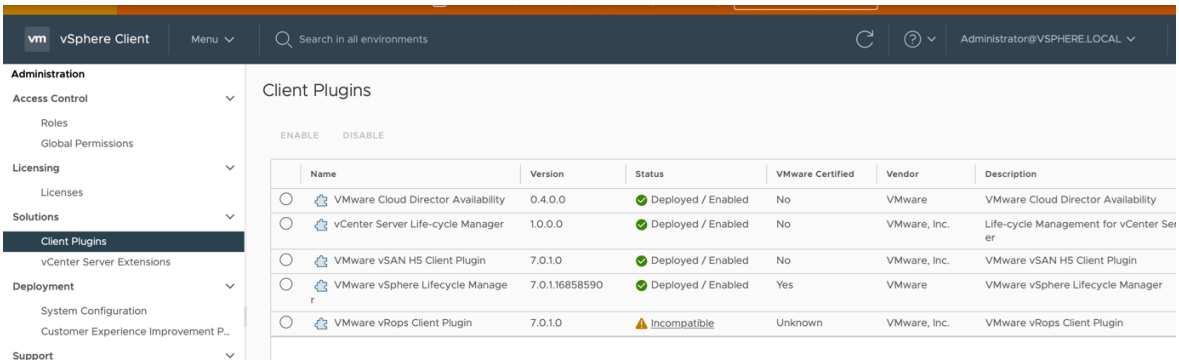
۵- به کمک مرورگر آدرس زیر را فراخوانی نمایید:

`https://<VC-IP-or-FQDN>/ui/vropspluginui/rest/services/checkmobregister`

در صورت انجام صحیح مراحل قبلی، مطابق تصویر شماره ۴ با خطای ۴۰۴/Not Found error مواجه خواهید شد.

تصویر ۴ : پیغام ۴۰۴ پس از تغییر و راه اندازی سرویس vsphere-ui

۶- با استفاده از رابط کاربری vSphere Client می توانید با مراجعه به بخش client-plugins از مسیر Administration > Solutions > client-plugins ، مطابق تصویر شماره ۵ حالت incompatible پلاگین VMware vROPS Client را مشاهده نمایید. این امر حاکی از غیرفعال شدن /ui/vropspluginui در سیستم میزبان می باشد.



تصویر ۵ : بررسی تغییر وضعیت پلاگینVMware vROPS CLient