Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI
GOBIERNO NACIONAL

BOLETÍN DE ALERTA

Boletín Nro.: 2021-02

Fecha de publicación: 25/02/2021

Tema: Vulnerabilidades críticas en productos de VMware.

Versiones afectadas:

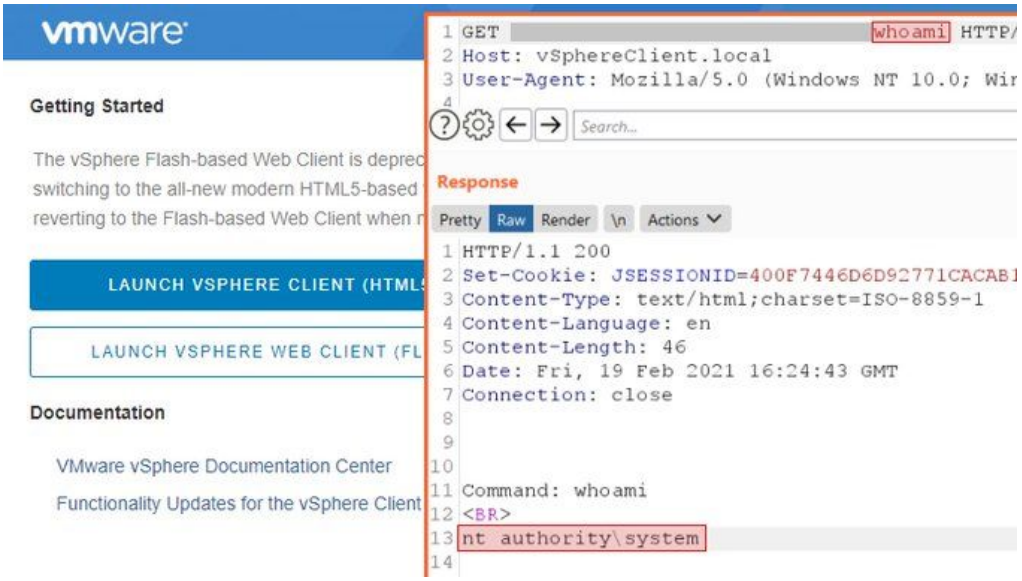
VMware vCenter Server versión 7.0, 6.7 y 6.5

VMware ESXi versión 7.0, 6.7 y 6.5

Descripción

VMware ha abordado varias vulnerabilidades críticas de ejecución remota de código (RCE) en la plataforma de administración de infraestructura virtual VMware ESXi y vSphere Client informadas por un equipo de investigadores de seguridad, que permitiría a los atacantes ejecutar comandos arbitrarios teniendo acceso a la red y al puerto 443 y hacerse con el control de los sistemas afectados, comunicó en un aviso la compañía.

El hipervisor VMware ESXi y el software de administración del servidor vCenter Server contienen un total de tres vulnerabilidades de seguridad, el más peligroso de los cuales está clasificado como crítico por el fabricante afectando a varias versiones y todas las plataformas disponibles se ven afectadas. Las actualizaciones de seguridad no solo están disponibles para ESXi y vCenter Server, sino también para la plataforma Cloud Foundation, que usa ambos como componentes



A continuación se describen las vulnerabilidades con sus respectivas severidad Crítica, Alta y Media

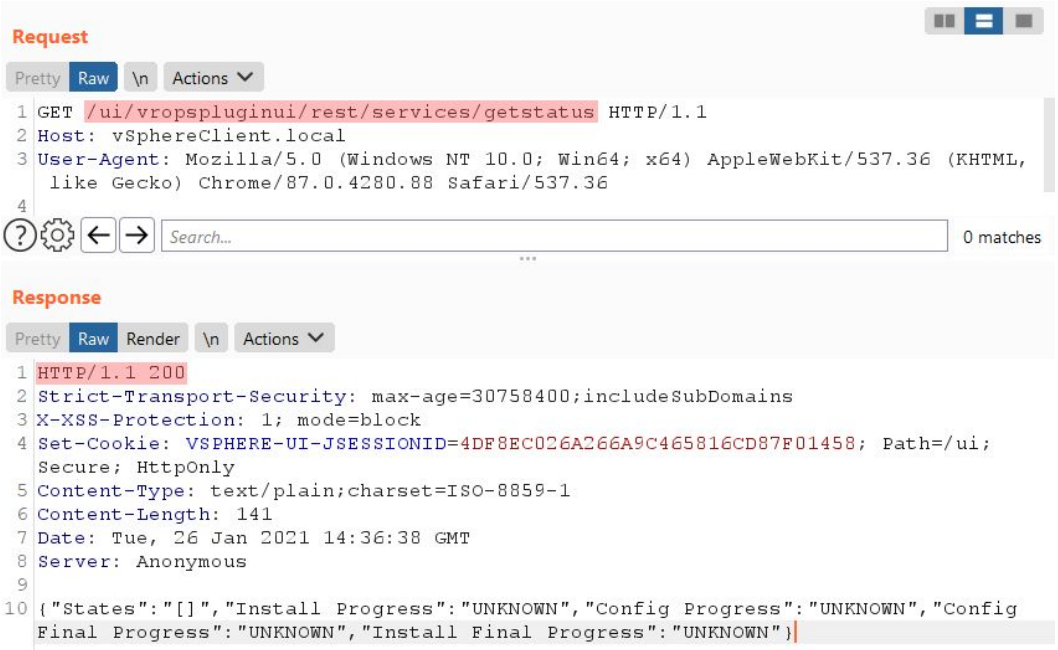
El CVE-2021-21972 severidad **crítica** y calificación **9,8** que afecta a vCenter Server y Cloud Foundation. Se encuentra en un complemento para vSphere Client basado en HTML5, que está activo de forma predeterminada en las instalaciones. Como consecuencia, un atacante remoto con acceso al puerto 443 podría, bajo ciertas condiciones, ejecutar comandos con permisos ilimitados en el respectivo sistema operativo subyacente.

Se encuentran afectados los productos VCenter Server en sus versiones 6.5, 6.7 y 7.0 , así como las series 3.xy 4.x de Cloud Foundation vulnerables .

El CVE-2021-21974 severidad Alta y calificación 8.8, que afecta a ESXi en sus versiones 6.5, 6.7 y 7.0 y Cloud Foundation, nuevamente en las series de versiones 3.xy 4.x. La ejecución remota de código es posible activando un desbordamiento de montón en el OpenSLP utilizado por ESXi a través del puerto 427. El ataque debe tener lugar desde el segmento de red utilizado por ESXi.

El CVE-2021-21973, de severidad Media y calificación 5.3, que afecta a vCenter Server y Cloud Foundation en las versiones ya mencionadas. Un atacante, con acceso de red al puerto 443, podría explotar una vulnerabilidad SSRF, generada por una validación incorrecta de las URL en un plugin de vCenter Server, enviando una solicitud POST a dicho plugin que podría causar una divulgación de información.

La vulnerabilidad se basa en la posibilidad de realizar una solicitud no autorizada a ***/ui/vropspluginui/rest/services/****, sin que sea requerida ninguna autenticación.



La aplicación web se basa en complementos, generalmente ubicados en archivos .jar separados, para algunas de sus funciones. El complemento vropspluginui, por ejemplo, se implementa en el archivo ***vropsplugin-service.jar***.

Por lo tanto cada complemento debe especificar cuáles de sus puntos finales requieren autorización en el panel web para ejecutarse y cuáles no. Este complemento está configurado para permitir que usuarios no autorizados accedan a cualquier URL que maneje la ***uploadOvaFile*** función, responsable de la URL ***/ui/vropspluginui/rest/services/uploadova***, creando un archivo .tar. Debido a la falta de filtrado del archivo .tar resultante, esto permite la creación arbitraria de archivos en ubicaciones arbitrarias en el servidor.
Actualmente se encuentra publicada en Internet una prueba de concepto así como exploits funcionales, aumentando el riesgo de la explotación masiva de estas vulnerabilidades

```java
@RequestMapping(value = {"/uploadova"}, method = {RequestMethod.POST})
public void uploadOvaFile(@RequestParam(value = "uploadFile", required = true) CommonsMultipartFile uploadFile,
HttpServletResponse response) throws Exception {
  //...
  if (!uploadFile.isEmpty())
    try {
      //...
      InputStream inputStream = uploadFile.getInputStream();
      File dir = new File("/tmp/unicorn_ova_dir");
      if (!dir.exists()) {
        dir.mkdirs();
      } else {
        String[] entries = dir.list();
        for (String str : entries) {
          File currentFile = new File(dir.getPath(), str);
          currentFile.delete();
        }
        logger.info("Successfully cleaned : /tmp/unicorn_ova_dir");
      }
      TarArchiveInputStream in = new TarArchiveInputStream(inputStream);
      TarArchiveEntry entry = in.getNextTarEntry();
      List<String> result = new ArrayList<String>();
      while (entry != null) {
        if (entry.isDirectory()) {
          entry = in.getNextTarEntry();
          continue;
        }
        File curfile = new File("/tmp/unicorn_ova_dir", entry.getName());
        File parent = curfile.getParentFile();
        if (!parent.exists())
          parent.mkdirs();
        OutputStream out = new FileOutputStream(curfile);
        IOUtils.copy((InputStream)in, out);
        out.close();
        result.add(entry.getName());
        entry = in.getNextTarEntry();
      }
      //...
}
```

Parte vulnerable del código.

Impacto

La fallas descritas podrían ser aprovechadas por atacantes remotos no autenticados sin la interacción del usuario, comprometiendo los sistemas que alojan los servicios, realizar escalado de privilegio y obtener información confidencial.

Solución y prevención

- Aplicar de forma inmediata los parches de seguridad según su producto afectado.

  - Para **vCenter 7.0** , aplique el parche **7.0U1c**, enlaces de notas de la versión.
  - Para **vCenter 6.7** , aplique el parche **6.7U3l**, enlace de notas de la versión.
  - Para **vCenter 6.5** , aplique el parche **6.5U3n**, enlace de notas de la versión.
  - Para **Cloud Foundation vCenter Server 4.x** , aplique el parche **4.2**.
  - Para **Cloud Foundation vCenter Server 3.x** , aplique el parche **3.10.1.2**.
  - Actualización para **vCenter Server 7.0.1**, documentación disponible.
  - Actualización para **vCenter Server 6.7 U3l**, documentación disponible.
  - Actualización para **vCenter Server 6.5 U3n**, documentación disponible.

- También existen otras soluciones y/o recomendaciones propuestas, en el siguiente enlace encontrará una tabla matriz en cuya columna "Soluciones alternativas" se encuentran listados algunas propuestas alternativas de solución.

Referencias

- https://www.vmware.com/security/advisories/VMSA-2021-0002.html
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-vmware-19
- https://www.ptsecurity.com/ww-en/about/news/vmware-fixes-dangerous-vulnerabilities-that-threaten-many-large-companies/
- https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-rce-bug-in-all-default-vcenter-installs/