BAN CƠ YẾU CHÍNH PHỦ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 193/BCY-CNTTGSM
V/v cảnh báo lỗ hổng bảo mật nghiêm trọng trên sản phẩm vCenter Server

Hà Nội, ngày 03 tháng 6 năm 2021

ĐẾN UBND TỈNH TRÀ VINH
Số: 923 ngày: 07/6/21
Chuyển: CN, LĐVP, LĐVP, các đ/v thuộc VP

Kính gửi:

- Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Đơn vị chuyên trách về CNTT Văn phòng Trung ương Đảng, Tỉnh ủy, Thành ủy, các Ban Đảng.

Thời gian qua, trong công tác giám sát an toàn thông tin, Ban Cơ yếu Chính phủ đã phối hợp với nhiều cơ quan đơn vị và xử lý các nguy cơ tấn công mạng, góp phần đảm bảo an toàn thông tin cho nhiều hệ thống mạng công nghệ thông tin trọng yếu của Đảng và Chính phủ.

Hiện nay, qua công tác giám sát, theo dõi có tồn tại lỗ hổng bảo mật mới trên sản phẩm vCenter Server (CVE 2021-21985), đây là lỗ hổng bảo mật được xác định là nghiêm trọng cho phép tin tặc có thể tấn công thực thi mã độc từ xa, từ đó kiểm soát và chiếm quyền điều khiển vCenter Server, lỗ hổng bảo mật này đã được công ty Vmware xác nhận trên trang chủ ngày 25/5/2021 (*Chi tiết tại Phụ lục kèm theo*).

Ban Cơ yếu Chính phủ thông báo và đề nghị Quý cơ quan kiểm tra, rà soát và cập nhật bản vá cho sản phẩm vCenter Server để phòng tránh nguy cơ tấn công mạng có thể xảy ra./.

Nơi nhận:
- Như trên;
- Đ/c Trưởng ban (để b/c);
- Lưu: VT, CNTTGSM. KC166.

KT. TRƯỞNG BAN
PHÓ TRƯỞNG BAN

Nguyễn Nam Hải

Phụ lục

THÔNG TIN VỀ CẢNH BÁO LỖ HỔNG CVE-2021-21985

(Kèm theo Công văn số 143/BCY-CNTTGSM ngày 03 tháng 6 năm 2021 của Ban Cơ yếu Chính phủ)

1. Mô tả

Theo khuyến cáo bảo mật VMSA 2021-0010 của công ty Vmware vào ngày 25/5/2021, trong đó có thông báo chi tiết đến lỗ hổng CVE-2021-21985 trong vSphere Client (HTML 5) một thành phần của vCenter Server và Vmware Cloud Foundation. Lỗ hổng phát sinh do lỗi xác thực thiếu kiểm tra tham số đầu vào trong tính năng của Virtual SAN Health Check (tính năng này được bật mặc định trong vCenter Server). Lỗ hổng này thực thi qua cổng 443 (https), cho phép kẻ tấn công thực hiện các lệnh với đặc quyền cao nhất trong hệ thống và không bị hạn chế bất kỳ truy cập nào đối với máy chủ cài hệ điều hành vCenter Server. Theo đánh giá của CVSSv3 mức độ nguy hiểm của CVE-2021-21985 là **9.8** (đặc biệt nghiêm trọng). Đây là nguy cơ có thể gây thiệt hại lớn đến các hệ thống của mạng của các cơ quan, đơn vị đang sử dụng hệ điều hành vCenter Server.

2. Các phiên bản bị ảnh hưởng

- vCenter Server 6.5
- vCenter Server 6.7
- vCenter Server 7.0
- Cloud Foundation (vCenter Server) 3.x
- Cloud Foundation (vCenter Server) 4.x

3. Bản vá

Thông tin về bản vá lỗ hổng theo đường link:
https://www.vmware.com/security/advisories/VMSA-2021-0010.html
Trong trường hợp đặc biệt nếu không thể vá ngay lập tức, quý cơ quan có thể tắt tính năng Virtual San Health Check tại đường dẫn:
https://kb.vmware.com/s/article/83829

4. IOCs

Để kiểm tra hệ thống bị tấn công bởi lỗ hổng CVE-2021-21985, có thể kiểm log trong các thư mục theo đường dẫn mặc định:

- vCenter Server 6.x và phiên bản cao hơn trên Windows server: *C:\ProgramData\VMware\vCenterServer\Logs*
- vCenter Server Appliance 6.x: */var/log/vmware/*
- vCenter Server Appliance 6.x flash: */var/log/vmware/vsphere-client*
- vCenter Server Appliance 6.x HTML5: */var/log/vmware/vsphere-ui*

hoặc theo cấu hình của người dùng có dấu hiệu như sau:

```
==> /var/log/vmware/vsphere-ui/logs/vsphere_client_virgo.log <==
[2021-05-28T15:45:14.391Z] [ERROR] http-nio-5090-exec-5          com.vmware.vsan.client.services.ProxygenController
service method failed to invoke org.eclipse.virgo.kernel.osgi.framework.ExtendedClassNotFoundException: CLASS cannot be
found by com.vmware.vsphere.client.h5vsan-6.7.0.20000-com.vmware.vsan.client.h5-vsan-service_6.5.0.11397901-storage-main in
KernelBundleClassLoader: [bundle=com.vmware.vsphere.client.h5vsan-6.7.0.20000-com.vmware.vsan.client.h5-vsan-
service_6.5.0.11397901-storage-main]
        at
org.eclipse.virgo.kernel.userregion.internal.equinox.KernelBundleClassLoader.loadClass(KernelBundleClassLoader.java:150)
        at java.lang.ClassLoader.loadClass(ClassLoader.java:357)
        at java.lang.Class.forName0(Native Method)
        at java.lang.Class.forName(Class.java:264)
        at com.vmware.vsan.client.services.ProxygenController.invokeService(ProxygenController.java:69)
        at sun.reflect.GeneratedMethodAccessor532.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:498)
        at org.springframework.web.method.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:205)
        at org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:133)
        at
org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandler
Method.java:97)
        at
org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandle
rAdapter.java:827)
        at
org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal(RequestMappingHandlerAdap
ter.java:738)
        at
org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHandlerMethodAdapter.java:85)
        at org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:967)
        at org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:901)
        at org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:970)
        at org.springframework.web.servlet.FrameworkServlet.doPost(FrameworkServlet.java:872)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:661)
        at org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:846)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:742)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:231)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)
        at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)
```

```
        at com.vmware.vise.security.SessionManagementFilter.doFilter(SessionManagementFilter.java:201)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)
        at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:198)
        at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:96)
        at org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:493)
        at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:140)
        at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:81)
        at org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:685)
        at org.eclipse.virgo.web.tomcat.support.ApplicationNameTrackingValve.invoke(ApplicationNameTrackingValve.java:33)
        at org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:650)
        at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:87)
        at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:342)
        at org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:800)
        at org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:66)
        at org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:800)
        at org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1471)
        at org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
        at org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
        at java.lang.Thread.run(Thread.java:748)
Caused by: java.lang.ClassNotFoundException: CLASS cannot be found by com.vmware.vsphere.client.h5vsan-6.7.0.20000-
com.vmware.vsan.client.h5-vsan-service_6.5.0.11397901-storage-main
        at org.eclipse.osgi.internal.loader.BundleLoader.findClassInternal(BundleLoader.java:501)
        at org.eclipse.osgi.internal.loader.BundleLoader.findClass(BundleLoader.java:421)
        at org.eclipse.osgi.internal.loader.BundleLoader.findClass(BundleLoader.java:412)
        at org.eclipse.osgi.internal.baseadaptor.DefaultClassLoader.loadClass(DefaultClassLoader.java:107)
        at
org.eclipse.virgo.kernel.userregion.internal.equinox.KernelBundleClassLoader.loadClass(KernelBundleClassLoader.java:146)
        ... 47 common frames omitted
```

5. Thông tin chi tiết

Thông tin chi tiết về lỗ hổng này có tại các đường link dưới đây:

- *https://www.vmware.com/security/advisories/VMSA-2021-0010.html*
- *https://blogs.vmware.com/vsphere/2021/05/vmsa-2021-0010.html*
- *https://core.vmware.com/resource/vmsa-2021-0010-faq*