安全事件通告

VMware 多个高危漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-02-24

报告信息

报告名称	VMware 多个高危漏洞通告		
报告类型	安全事件通告	**报告编号**	B6-2021-022401
报告版本	1	**报告日期**	2021-02-24
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-02-24	360CERT	360CERT	撰写报告

目录

一、 事件档案

漏洞类型	溢出
CVE 编号	CVE-2021-21974 等
相关厂商	VMware
相关组件	暂无
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案/临时修补方案
事件发布时间	2021-02-24
报告生成时间	2021-02-24

二、 事件简述

2021 年 02 月 24 日，360CERT 监测发现 VMware 发布了 Vcenter Server、ESXI 的风险通告，事件等级：严重，事件评分：9.8。

VMware 更新了 ESXI 和 vSphere Client(HTML5)中的两个高危漏洞，具有网络端口访问权限的恶意攻击者可以通过漏洞执行任意代码。

对此，360CERT 建议广大用户及时将 Vcenter Server 与 ESXI 产品升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、 事件评级

经过安全技术人员的分析，最终对该事件的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、 事件详情

CVE-2021-21972：代码执行漏洞

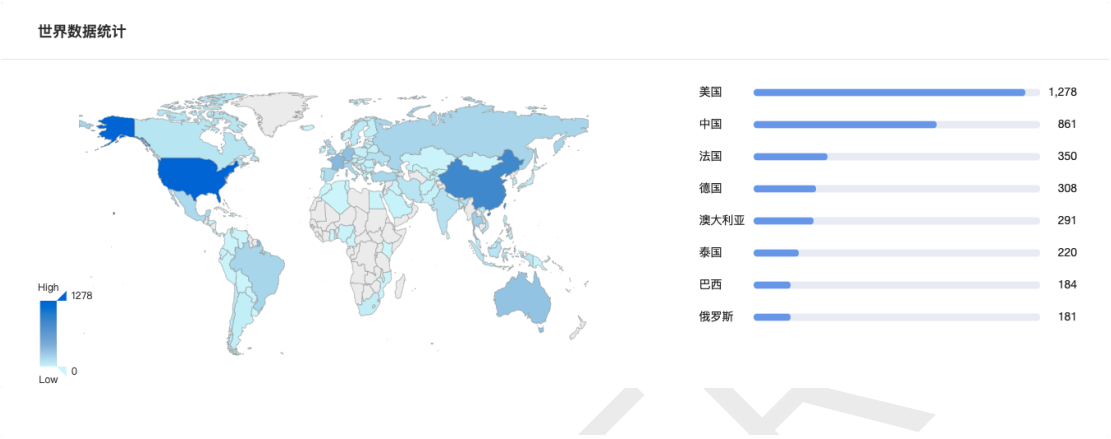
具有 443 端口访问权限的恶意攻击者可以通过向 vCenter Server 发送精心构造的请求，最终造成远程任意代码执行。

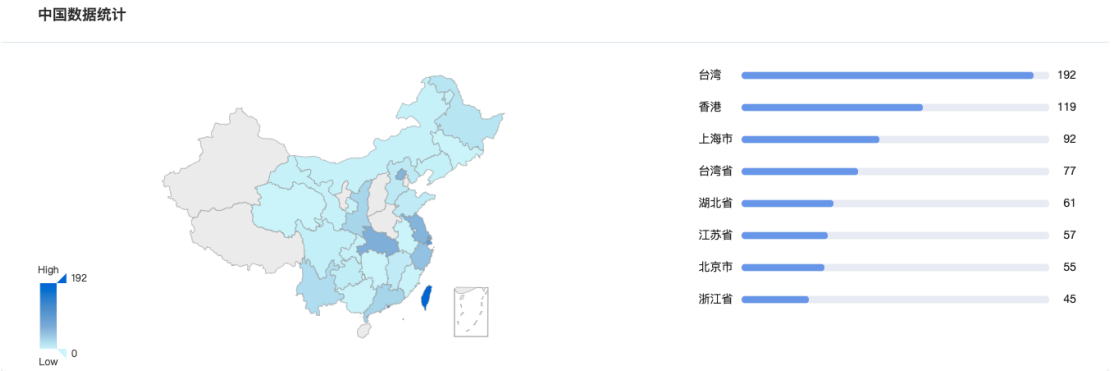
CVE-2021-21974：堆溢出漏洞

与 ESXI 处于同一网段且可以访问 427 端口的恶意攻击者可以构造恶意请求包触发 OpenSLP 服务中的堆溢出漏洞，最终造成远程代码执行。

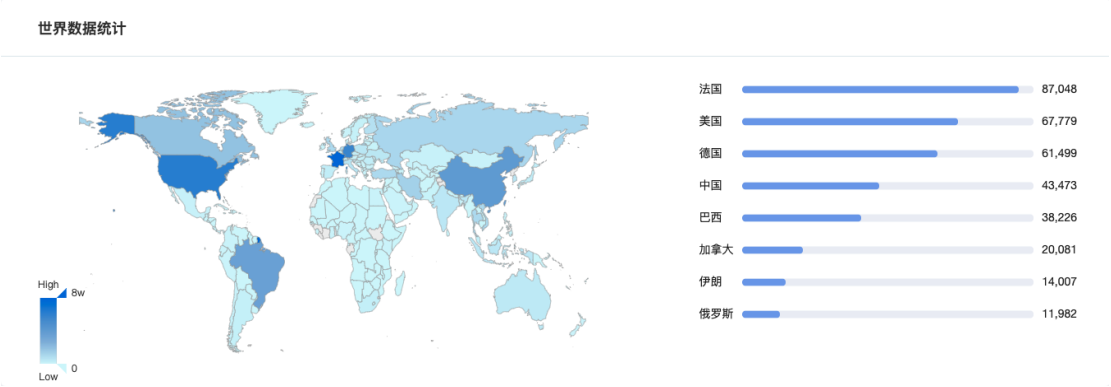
五、 相关空间测绘数据

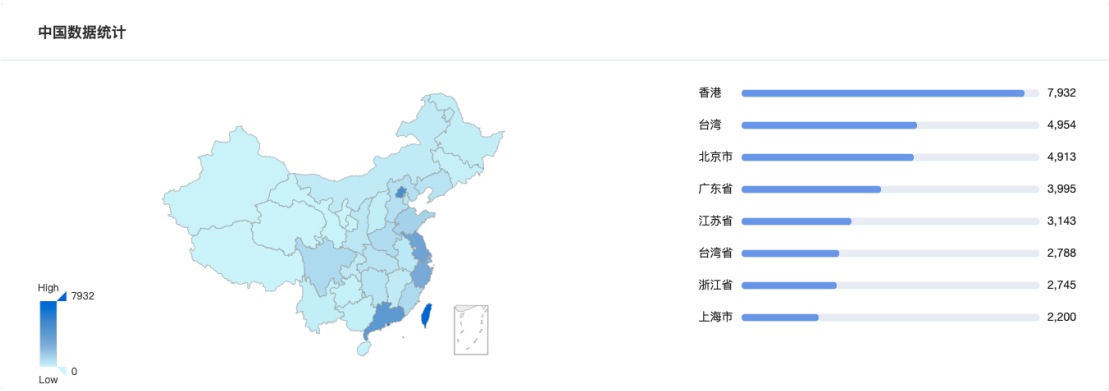
360 安全大脑-Quake 网络空间测绘系统通过对全网资产测绘，发现 vCenter Server 具体分布如下图所示。





ESXI 具体分布如下图所示。





六、 影响版本

产品名称	影响版本
esxi	7.0
esxi	6.7
esxi	6.5
vcenter_server	7.0
vcenter_server	6.7
vcenter_server	6.5

七、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-21974	溢出	任意代码执行	高危
CVE-2021-21972	代码执行	任意代码执行	严重

八、 安全建议

(一) 通用修补方案

- 针对 CVE-2021-21972:

- vCenter Server7.0 版本升级到 7.0.U1c

- vCenter Server6.7 版本升级到 6.7.U3l

- vCenter Server6.5 版本升级到 6.5 U3n

- 针对 CVE-2021-21974:

- ESXi7.0 版本升级到 ESXi70U1c-17325551

- ESXi6.7 版本升级到 ESXi670-202102401-SG

- ESXi6.5 版本升级到 ESXi650-202102101-SG

(二) 临时修补方案

CVE-2021-21972

1. SSH 远连到 vCSA（或远程桌面连接到 Windows VC）

2. 备份以下文件:

- Linux 系文件路径为：/etc/vmware/vsphere-ui/compatibility-matrix.xml (vCSA)

- Windows 文件路径为：C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui (Windows VC)

3. 使用文本编辑器将文件内容修改为:

4. 使用 vmon-cli -r vsphere-ui 命令重启 vsphere-ui 服务

5. 访问 https://<VC-IP-or-FQDN>/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

CVE-2021-21974

1. 使用/etc/init.d/slpd stop 命令在 ESXI 主机上停止 SLP 服务（仅当不使用 SLP 服务时，才可以停止该服务。可以使用 esxcli system slp stats get 命令查看服务守护程序运行状态）

2. 使用 esxcli network firewall ruleset set -r CIMSLP -e 0 命令禁用 SLP 服务

3. 使用 chkconfig slpd off 命令保证此更改在重启后持续存在

4. 利用 chkconfig --list | grep slpd 命令检查是否在重启后更改成功，若回显为 slpd off 则证明成功

九、 产品侧解决方案

(一) 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台(quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。

十、 参考链接

1. VMware 官方安全通告

   https://www.vmware.com/security/advisories/VMSA-2021-0002.html

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危