CVE-2020-3960 | VMware 多个产品信息泄露漏洞通告

0x00 漏洞概述

产品	CVE ID	类 型	漏洞等级	远程利用	影响范围
VMware vSphere ESXi (ESXi)	CVE-2020-3960	ROB	严重	是	ESXi 6.5、6.7
VMware Workstation Pro / Player (Workstation)	CVE-2020-3960	ROB	严重	是	Workstation 15.x
VMware Fusion Pro / Fusion (Fusion)	CVE-2020-3960	ROB	严重	是	Fusion 11.x

0x01 漏洞详情

VMware 虚拟机软件，是全球桌面到数据中心虚拟化解决方案的领导厂商。全球不同规模的客户依靠 VMware 来降低成本和运营费用、确保业务持续性、加强安全性并走向绿色。2020 年 6 月 9 日 VMware 发布安全更新，修复了 VMware ESXi、Workstation 和 Fusion 产品中的多个安全漏洞，具体信息如下：

Vmware ESXi、Workstation 和 Fusion 产品中的 NVMe 功能中包含越界读取漏洞（CVE-2020-3960）。攻击者可以利用该漏洞以非管理员身份访问虚拟机并从内存中读取特权信息。

NVMe（Nonvolatile Memory Express，非易失性内存标准）是一种闪存和下一代固态驱动器（SSD）的全新存储访问和传输协议，可为所有类型的企业工作负载提供最高的吞吐量和最快的响应速度。

0x02 处置建议

VMware 已经发布上述漏洞的补丁，但是没有提供解决方法。

ESXi 6.7 补丁程序 ESXi670-202006401-SG

https://my.vmware.com/group/vmware/patch

https://docs.vmware.com/en/VMware-vSphere/6.7/rn/ESXi670-202006401-SG.html

ESXi 6.5 补丁程序 ESXi650-202005401-SG

https://my.vmware.com/group/vmware/patch

https://docs.vmware.com/en/VMware-vSphere/6.5/rn/ESXi650-202005401-SG.html

VMware Workstation Pro 15.5.5

https://www.vmware.com/go/downloadworkstation

https://docs.vmware.com/cn/VMware-Workstation-Pro/index.html

VMware Fusion 11.5.5

https://www.vmware.com/go/downloadfusion

https://docs.vmware.com/cn/VMware-Fusion/index.html

0x03 相关新闻

https://securityaffairs.co/wordpress/104579/security/vmware-products-flaw.html?utm_source=rss&utm_medium=rss&utm_campaign=vmware-products-flaw

0x04 参考链接

https://www.vmware.com/security/advisories/VMSA-2020-0012.html

0x05 时间线

2020-06-09 VMware 发布漏洞公告
2020-06-11 VSRC 发布漏洞通告