بسمه تعالی

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

وصله آسیب‌پذیرهای با شدت بالا در VMware Workstation، Fusion و vSphere

خبر آسیب‌پذیری

شناسه سند ..... Maher_11983

نوع سند ..... گزارش فنی

شماره نگارش ۱

تاریخ نگارش ۱۳۹۹/۰۳/۲۵

طبقه‌بندی سند ..... عادی

تهران- میدان آرژانتین- ابتدای بلوار بیهقی- نبش خیابان شانزدهم- ساختمان شماره ۱ سازمان فناوری اطلاعات ایران

(۰۲۱)۴۲۶۵۰۰۰۰

۴۲۶۵۰۰۰۰ ۰۲۱

cert.ir

بر اساس گزارشات منتشر شده، VMware چند آسیب‌پذیری با شدت بالا را وصله کرده است که بر روی چندین محصول این شرکت تاثیر می‌گذارد و بهره‌برداری از آنها به مهاجمان اجازه می‌دهد تا به اطلاعات حساس دست یابند.

۱-۱ شرح آسیب‌پذیری‌ها

۱-۱-۱ CVE-2020-3960

یکی از آسیب‌پذیری‌های وصله شده که با شناسه " CVE-2020-3960 " شناخته می‌شود، یک آسیب‌پذیری خواندن out-of-bounds می‌باشد که VMware ESXi، Workstation و Fusion را تحت تاثیر قرار می‌دهد. به کاربران توصیه می‌شود که نرم‌افزارهای فوق را به نسخه‌های وصله شده بروز نمایند. این نقص در عملکرد NVMe قرار دارد. NVMe (nonvolatile memory express) یک پروتکل جدید دسترسی به storage و انتقال برای فلش و SSDs است که بالاترین توان و سریعترین زمان پاسخگویی را برای تمام حجم کاری سازمان ارائه می‌دهد. به موجب این آسیب‌پذیری، مهاجم با دسترسی لوکال و non-administrative به یک ماشین مجازی، ممکن است بتواند اطلاعات ویژه و خاص موجود در حافظه را بخواند.

جدول1 : محصولات آسیب‌پذیر و وصله شده برای آسیب‌پذیری CVE-2020-3960

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
ESXi	**7.0**	**Any**	**CVE-2020-3960**	**N/A**	**N/A**	**Unaffected**	**N/A**	**N/A**
ESXi	6.7	Any	CVE-2020-3960	7.1	Important	ESXi670-202006401-SG	None	None
ESXi	6.5	Any	CVE-2020-3960	7.1	Important	ESXi650-202005401-SG	None	None
Workstation	15.x	Any	CVE-2020-3960	7.1	Important	15.5.5	None	None
Fusion	11.x	Any	CVE-2020-3960	7.1	Important	11.5.5	None	None

۱-۱-۲ CVE-2020-3961

نقص بعدی یک آسیب‌پذیری ارتقاء سطح دسترسی است که در VMware Horizon Client مربوط به سیستم‌عامل ویندوز وجود دارد و ناشی از پیکربندی مجوزهای دسترسی و بارگذاری ناامن کتابخانه‌ها می‌باشد.

آسیب‌پذیری مذکور می‌تواند توسط یک کاربر لوکال در سیستم، مورد سوءاستفاده قرار گیرد و پس از آن به عنوان هر کاربر دیگری دستورات را اجرا نماید.

این آسیب‌پذیری بر روی Horizon Client 5.x مخصوص ویندوز تاثیر می‌گذارد و پیش از این، در نسخه ۵,۴,۳ وصله شده است. به این آسیب‌پذیری شدت important و CVSSv3 8.4 اختصاص داده شده است.

جدول2: محصولات آسیب‌پذیر و وصله شده برای آسیب‌پذیری CVE-2020-3961

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
Horizon Client for Windows	5.x and prior	Windows	CVE-2020-3961	8.4	Important	5.4.3	None	None

۱-۱-۳ CVE-2020-3956

آسیب‌پذیری بعدی یک آسیب‌پذیری تزریق کد در VMware Cloud Director است که منجر به اجرای کد از راه دور می‌شود. این آسیب‌پذیری می‌تواند با ارسال ترافیک مخرب به VMware Cloud Director و از طریق HTML5 و Flex-based UIs، API Explorer interface و دسترسی API مورد اکسپلویت قرار گیرد.

VMware Cloud Director یک بستر ارئه‌دهنده خدمات ابری است که به سازمان‌ها امکان می‌دهد تا کسب و کارهای سرویس ابری را مدیریت و اجرا کنند.

این آسیب‌پذیری به طور بالقوه می‌تواند به یک مهاجم احراز هویت شده امکان دسترسی به شبکه شرکت‌ها، دسترسی به داده‌های حساس و کنترل فضای ابری محرمانه را در تمام زیرساخت‌ها فراهم کند.

جدول3: محصولات آسیب‌پذیر و وصله شده برای آسیب‌پذیری CVE-2020-3956

Product	Version	Running On	CVE Identifier	CVSSV3	Severity	Fixed_Version	Workarounds	Additional Documentation
VMware Cloud Director	**10.1.0**	**Linux, PhotonOS appliance**	**CVE-2020-3956**	**N/A**	**N/A**	**Not affected**	**N/A**	**N/A**
vCloud Director	10.0.x	Linux, PhotonOS appliance	CVE-2020-3956	8.8	Important	10.0.0.2	KB79091	None
vCloud Director	9.7.x	Linux, PhotonOS appliance	CVE-2020-3956	8.8	Important	9.7.0.5	KB79091	None
vCloud Director	9.5.x	Linux, PhotonOS appliance	CVE-2020-3956	8.8	Important	9.5.0.6	KB79091	None

Product	Version	Running On	CVE Identifier	CVSSV3	Severity	Fixed_Version	Workarounds	Additional Documentation
vCloud Director	9.1.x	Linux	CVE-2020-3956	8.8	Important	9.1.0.4	KB79091	None
vCloud Director	9.0.x	Linux	CVE-2020-3956	N/A	N/A	Not affected	N/A	N/A
vCloud Director	8.x	Linux	CVE-2020-3956	N/A	N/A	Not affected	N/A	N/A

۱-۲ راه‌حل

با توجه به اهمیت آسیب‌پذیری‌های ذکر شده و نیز عمومیت استفاده از نرم‌افزارهای فوق، توصیه می‌شود کاربران هر چه سریعتر نسبت به بروزرسانی محصولات آسیب‌پذیر اقدام نمایند.

۱-۳ منابع:

https://gbhackers.com/vmware-fixes-high-severity-flaw-that-affects-vmware-workstation-fusion-and-vsphere-products/

https://securityaffairs.co/wordpress/104579/security/vmware-products-flaw.html

https://www.vmware.com/security/advisories/VMSA-2020-0010.html

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

https://www.vmware.com/security/advisories/VMSA-2020-0013.html