Zranitelnost typu Use-After-Free v produktech společnosti VMware

portal.nukib.gov.cz/informacni-servis/informace/upozorneni-a-hrozby/zranitelnost-typu-use-afer-free-v-produktech-vmware

Chtěli bychom vás upozornit na kritickou zranitelnost v produktech společnosti VMware, která může vést ke spuštění škodlivého kódu přímo na zařízeních, kde je virtualizační software nainstalován. Tato zranitelnost je kritická pro produkty VMware Workstation Pro a Player a VMware Fusion. U produktů VMware vSphere od verze 7 a vyšší není riziko tak vysoké vzhledem k implementovaným bezpečnostním opatřením v rámci ESXi, které tento produkt obsahuje. To nicméně neplatí pro vSphere verze 6, kde je riziko stejně vysoké jako u desktopových produktů.

Ke zneužití této zranitelnosti potřebuje útočník oprávnění na úrovni lokálního administrátora virtuálního stroje, který běží na některé ze zmíněných virtualizačních platforem.

- CVE-2024-22252 Use After Free (9.3) - VMware Workstation Pro & Player, VMWare Fusion a VMware ESXi
- CVE-2024-22253 Use After Free (9.3) - VMware Workstation Pro & Player, VMWare Fusion a VMware ESXi

Aktualizace těchto produktů mitigující zmíněné zranitelnosti jsou již k dispozici. Proto tyto produkty aktualizujte bez zbytečného odkladu. V rámci mitigace je možné ještě odebrat USB řadiče virtuálních strojů, které tato zranitelnost zneužívá. Nicméně jak autoři software uvádějí, může toto omezit funkcionality jiných nástrojů (např. VM console).

Zdroje

- https://www.vmware.com/security/advisories/VMSA-2024-0006.html
- https://core.vmware.com/resource/vmsa-2024-0006-questions-answers

Klasifikace

TLP:CLEAR

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

06. 03. 2024

Obsah

Reakce

Zatím žádné reakce na článek