Kalteberatasun kritikoak VMware ESXi, Workstation eta Fusionen

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

EDUKI-TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau Zibersegurtasunaren Euskal Agentziak erakundeen eta herritar interesatuen segurtasunaren alde beharrezkotzat jotzen dituen alertak gizarteratzeko helburuz sortu da. Zibersegurtasunaren Euskal Agentzia ezin da jo, inola ere, Zibersegurtasunerako Euskal Agentziaren webgunean emandako informazioaren edo erreferentzia egiten zaien teknologien erabilerak eragin ditzaketen kalteen erantzuletzat, ezta kanpoko web-orrialdeetarako esteka bidez sartutako bestelako informazioaren, software produktuen edo Zibersegurtasunaren Euskal Agentziaren webgunean edo alertan ager daitezkeen beste edozein informazioaren erantzuletzat ere. Edonola ere, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak iritzi eta gomendioak dira, hemen bildutako terminoekin bat etorrita, eta emandako informazioaren ondorioz ezingo da eragin juridiko loteslerik sortu.

Salmenta debekatzeko klausula

1. Laburpen exekutiboa

VMwarek segurtasun-abisu bat argitaratu du **larritasun kritikoa** duten **4 kalteberatasunekin** lotuta. Honako identifikatzaileak dituzte: CVE-2024-22252, CVE-2024-22253, CVE-2024-22254 eta CVE-2024-22255. Eta **VMware ESXi, Workstation eta Fusion** produktuei eragiten diete. Akats horiek Use-After-Free baldintzak, mugez kanpoko idazketa eta **informazioaren hedapena** eragiten dituzte. Hala, akatsik larrienak mehatxu oso larriak dira, eta eragina dute kaltetutako sistemen konfidentzialtasunean, segurtasunean eta eskuragarritasunean.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak eta arintze-neurriak, eta, horrela, akats nabarmenak zuzendu ditu. Beraz, kalteberatasun horiek eta beste batzuk prebenitzeko, sistema eta aplikazioak eskuragarri dagoen azken bertsioaren arabera eguneratuta izatea gomendatzen da, dagozkien adabakiak argitaratu bezain laster.

2. Kaltetutako baliabideak

- VMware ESXi: 7.0 eta 8.0 bertsioak
- VMware Workstation Pro / Player: 17.x bertsioak.
- VMware Fusion Pro / Fusion: 13.x bertsioak.
- VMware Cloud Foundation: 5.x/4.x bertsioak.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2024-22252: Use-After-Free kalteberatasuna VMware ESXi, Workstation eta Fusionen, USB XHCI kontroladorean. Makina birtual batean tokiko pribilegio administratiboak dituen aktore gaizto batek arazo hori aprobetxatu dezake kodea exekutatzeko, hostean exekutatzen ari den makina birtualaren VMX prozesu gisa. ESXi-n, ustiapena VMXeko sandboxaren barruan dago. Workstationen eta Fusionen kasuan, berriz, Workstation edo Fusion instalatuta dagoen makinan exekutatu daiteke kodea.

Kalteberatasunen azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **8.4**

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Eraso-bektorea:** Bertakoa
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: **Aldaketekin**
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2024-22253: Use-After-Free kalteberatasuna VMware ESXi, Workstation eta Fusionen, USB XHCI kontroladorean. Makina birtual batean tokiko pribilegio administratiboak dituen asmo txarreko aktore batek arazo hori aprobetxatu dezake kodea exekutatzeko, hostean exekutatzen ari den makina birtualaren VMX prozesu gisa. ESXi-n, ustiapena VMXeko sandboxaren barruan dago. Workstationen eta Fusionen kasuan, berriz, Workstation edo Fusion instalatuta dagoen makinan exekutatu daiteke kodea.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **8.4**

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Eraso-bektorea:** Bertakoa
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: **Aldaketekin**
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**

- **Eskuragarritasuna: Altua**

CVE-2024-22254: mugez kanpoko idazketa kalteberatasuna, VMware ESXi-n. VMX prozesuaren barruan pribilegioak dituen asmo txarreko aktore batek mugez kanpoko idazketa eragin dezake, eta horrek sandboxetik irtetea eragin dezake.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **7.9**

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

- **Eraso-bektorea:** Bertakoa
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak:** Altuak
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: **Aldaketekin**
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna:** Bat ere ez

CVE-2024-22255: informazioa hedatzeko kalteberatasuna VMware ESXi, Workstation eta Fusionen, USB UHCI kontroladorean. Makina birtual baterako sarbidea duen asmo txarreko aktore batek arazo hori aprobetxatu lezake vmx prozesutik memoria filtratzeko.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **7.1**

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

- **Eraso-bektorea:** Bertakoa
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: **Aldaketekin**
- **Konfidentzialtasuna Altua**
- **Integritatea:** Bat ere ez
- **Eskuragarritasuna:** Bat ere ez

4. Arintzea / Konponbidea

Ohikoa den bezala, kalteberatasun horiek eta beste batzuk prebenitzeko, sistemak eta aplikazioak beti eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, dagozkien eguneratzeak argitaratu bezain laster.

Kalteberatasun horiei erantzuteko, zuzendutako bertsioetara eguneratzeko gomendatzen die VMwarek bere bezeroei. Honako hauek dira zuzendutako bertsioak:

- ESXi 8.0ren kasuan, eguneratu hona: ESXi80U2sb-23305545.
- ESXi 8.0 [2]-ren kasuan, eguneratu hona: ESXi80U1d-23299997.
- ESXi 7.0ren kasuan, eguneratu hona: ESXi70U3p-23307199.
- Workstation 17.x-ren kasuan, eguneratu 17.5.1. bertsiora.
- Fusion 13.x-ren kasuan, eguneratu 13.5.1. bertsiora.
- Cloud Foundation (ESXi) 5.x/4.x-ren kasuan, eguneratu KB88287-ra.

Gainera, kalteberatasun guztien kasuan, arintzeko modu alternatiboak eskaintzen ditu VMwarek. Honako esteka honetan eskuratu daitezke.

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-22252.
- CVE-2024-22253.
- CVE-2024-22254.
- CVE-2024-22255.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY