TLP:CLEAR
Szabadon terjeszthető!

Riasztás
Palo Alto, VMware és Fortinet termékek sérülékenységeiről

(2024. november 21.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztást** ad ki **kritikus** kockázati besorolású sérülékenységekről **Palo Alto** tűzfalak, **VMware vCenter** szerverszoftverek, valamint a **Fortinet VPN klienst érintően**, a termékek széles körű elterjedtsége, a sebezhetőségek súlyossága, kihasználhatósága miatt.

Mindhárom termék esetében ismert az aktív kihasználás, ezért az NBSZ NKI javasolja a sérülékeny rendszerek haladéktalan frissítését.

A Palo Alto Networks tűzfalak PAN-OS operációs rendszerét **kritikus** kockázati besorolású sérülékenység érinti (CVE-2024-0012), amely az Internet felől elérhető webes management interfészen keresztül kihasználható. A sebezhetőség illetéktelenek számára lehetővé teheti a hitelesítés megkerülését, valamint további sérülékenységek kihasználását (például a CVE-2024-9474 azonosítójú sebezhetőséget jogosultság-kiterjesztésre) ami teljes rendszer-kompromittálódáshoz vezethet.

Termék:	Érintett verziók:	Javított verzió:	Gyártói biztonsági közlemény:
Palo Alto Networks **PAN-OS 10.2,** **PAN-OS 11.0,** **PAN-OS 11.1,** **PAN-OS 11.2** **(PA-, VM-, CN szériás tűzfal termékek, mind Panorama, mind M-szériás és WildFire appliance-eken).**	**< 11.2.4-h1** **< 11.1.5-h1** **< 11.0.6-h1** **< 10.2.12-h2**	**>= 11.2.4-h1** **>= 11.1.5-h1** **>= 11.0.6-h1** **>= 10.2.12-h2**	**PAN-SA-2024-0015**

Támadásra utaló indikátorok elérhetők itt: https://unit42.paloaltonetworks.com/cve-2024-0012-cve-2024-9474/

TLP:CLEAR
Szabadon terjeszthető!

Broadcom új biztonsági frissítéseket adott ki több kritikus sérülékenység javításához. A biztonsági hibák között a CVE-2024-38812, valamint a CVE-2024-38813 sérülékenységek a legsúlyosabbak, előbbi távoli kódfuttatást, utóbbi jogosultság-kiterjesztést tehet lehetővé.

Termék:	Érintett verziók:	Javított verzió:	Gyártói biztonsági közlemény:
VMware vCenter Server, **VMware Cloud Foundation**	**vCenter 8.0, 7.0** **VMware Cloud Foundation 5.x, 5.1.x, 4.x**	**8.0 U3d** **8.0 U2e** **7.0 U3t**	(**VMSA-2024-0019**) Async patch guide az upgrade-hez: **KB88287**

A **Fortinet FortiClient Windows VPN** kliens zero-day sérülékenysége, amely még nem rendelkezik CVE azonosítóval. Amíg a Fortinet nem ad ki biztonsági frissítést, javasolt korlátozni a VPN-hozzáférést, és figyelni a szokatlan bejelentkezéseket.

Termék:	Érintett verziók:	Javított verziók	Gyártói biztonsági közlemény:
Fortinet FortiClient Windows VPN kliens	**Jelenleg nincs gyártói közlemény**	**Jelenleg nem érhető el gyártói javítás**	-

Támadásra utaló indikátorok elérhetők itt: https://github.com/volexity/threat-intel/blob/main/2024/2024-11-15%20BrazenBamboo/iocs.csv

Hivatkozások:

- https://nki.gov.hu/it-biztonsag/hirek/kritikus-palo-alto-tuzfal-sebezhetosegek-kerultek-javitasra/
- https://nki.gov.hu/it-biztonsag/hirek/kritikus-vmware-vcenter-serulekenyseg-aktiv-kihasznalas-alatt/
- https://nki.gov.hu/it-biztonsag/hirek/fortinet-vpn-ek-elleni-tamadast-azonositott-a-volexity/

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu