Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0269

Kwetsbaarheden verholpen in VMware ESXi en vCenter Server

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 30-07-2024
Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

Onderzoekers bij Microsoft melden dat de kwetsbaarheid met kenmerk CVE-2024-37085 misbruikt wordt om ransomware te installeren op kwetsbare eSXI systemen. Achtergrondartikel toegevoegd. Omdat misbruik voorafgaande rechten vereist wijzigt de inschaling verder niet.

Feiten

VMware heeft kwetsbaarheden verholpen in ESXi en vCenter Server.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service op de host te veroorzaken, of om zichzelf verhoogde rechten toe te kennen en zo handelingen uit te voeren waarvoor de kwaadwillende aanvankelijk niet is geautoriseerd. Hiervoor dient de kwaadwillende wel bepaalde rechten te hebben in de Active Directory welke voor autorisaties wordt gebruikt.

Onderzoekers bij Microsoft melden actief misbruik waar te nemen van de kwetsbaarheid met kenmerk CVE-2024-37085, waarbij ransomware wordt geïnstalleerd. Succesvol misbruik vereist voorafgaande authenticatie en autorisatie.

Oplossingen

VMware heeft updates uitgebracht om de kwetsbaarheden te verhelpen in ESXi en vCenter Server. Zie bijgevoegde referenties voor meer informatie.

Referenties

› https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505
› https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/

Kwetsbaarheden

CVE	CVSS Score
› CVE-2024-37085	

CVE-2024-37086	**6.8 MEDIUM**
CVE-2024-37087	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-125	Out-of-bounds Read
CWE-287	Improper Authentication
CWE-404	Improper Resource Shutdown or Release

Getroffen producten

n_a
esxi
vcenter_server
vmware_cloud_foundation
vmware_esxi
vmware
cloud_foundation
esxi
vcenter_server

Disclaimer