Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0377

Kwetsbaarheden verholpen in VMware vCenter Server

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-11-2024
Revisie: 1.0.2

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 2

VMWare heeft aangegeven dat de patches die op 17 september 2024 zijn gepubliceerd niet voldoende zijn om de kwetsbaarheid van CVE-2024-38812 te verhelpen. Hiervoor is een nieuwe update beschikbaar gekomen. Zie bijgevoegde referenties voor meer informatie.

Feiten

VMware heeft kwetsbaarheden verholpen in vCenter Server.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen, mogelijk zelfs tot root en willekeurige code uit te voeren op het systeem.

VMware meldt in een update van het originele beveiligingsadvies dat misbruik is waargenomen. Details over de omvang en gevolgen worden verder niet gegeven.

Oplossingen

VMware heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Update: VMWare heeft aangegeven dat de patches die op 17 september 2024 zijn gepubliceerd niet voldoende zijn om de kwetsbaarheid van CVE-2024-38812 te verhelpen. Hiervoor is een nieuwe update beschikbaar gekomen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968
- https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u3s-release-notes/index.html
- https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u3b-release-notes/index.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-38812	9.8 CRITICAL
CVE-2024-38813	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-273	Improper Check for Dropped Privileges
CWE-250	Execution with Unnecessary Privileges
CWE-122	Heap-based Buffer Overflow

Getroffen producten

n_a
vmware_cloud_foundation
vmware_vcenter_server
vmware
cloud_foundation
vcenter_server

Disclaimer