



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

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.