Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0510

PRIORITEIT: HOOG

Kwetsbaarheden verholpen in VMware-producten

Publicatiedatum: 20-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

VMware heeft kwetsbaarheden verholpen in VMware vCenter Directory Service, VMware Telco Cloud Platform, VMware SDDC Manager en VMware Tools voor Windows.

Duiding

De kwetsbaarheden betreffen meerdere VMware-producten en versies. In VMware vCenter Directory Service en VMware Telco Cloud Platform kunnen authenticatiemechanismen worden omzeild, waardoor ongeautoriseerde toegang mogelijk is. VMware SDDC Manager bevat meerdere kwetsbaarheden: een SQL-injectie door onvoldoende sanitatie van gebruikersinvoer, een command-injectie waarbij een geauthenticeerde gebruiker willekeurige commando's kan uitvoeren, en een lokale privilege-escalatie waarmee een gebruiker met lokale toegang zijn rechten kan verhogen. VMware Tools voor Windows heeft een kwetsbaarheid waarbij de handtekeningverificatie van SAML-tokens kan worden omzeild, wat invloed heeft op authenticatiemechanismen. De kwetsbaarheden zijn aanwezig in specifieke versies van de genoemde producten.

De kwetsbaarheid met kenmerk CVE-2026-123890 wordt al actief misbruikt.

Oplossingen

VMware heeft updates uitgebracht voor de betrokken producten en versies om deze kwetsbaarheden te verhelpen. Voor SDDC Manager zijn de kwetsbaarheden verholpen in versies 9.1.1.0200, 9.0.2.0100 en 5.2.5. Voor VMware Tools voor Windows zijn de kwetsbaarheden verholpen in versies 13.1.5.0 en 12.5.5. Zie de referenties voor meer informatie.

Referenties

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39495

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-123890	9.8 CRITICAL
CVE-2026-123891	8.1 HIGH
CVE-2026-123892	7.2 HIGH
CVE-2026-123893	6.7 MEDIUM
CVE-2026-123894	6.7 MEDIUM

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-89	Improper Neutralization of Special Elements used in an SQL Command
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-347	Improper Verification of Cryptographic Signature

Getroffen producten

VMware
Cloud Foundation
Telco Cloud Infrastructure
Telco Cloud Platform
Tools
VMware Tools
VMware vCenter

VMware
Vcenter Server
tools
vCenter
vSphere Foundation

vmware
sddc_manager
vcf_installer

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.