Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0523

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in VMware vCenter en aanverwante producten

Publicatiedatum: 26-11-2026

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 meerdere kwetsbaarheden verholpen in VMware vCenter Server, VMware Cloud Foundation, VMware Telco Cloud Platform, VMware ESX, ESXi, Fusion en VMware Tools.

Duiding

De kwetsbaarheden betreffen onder andere een bypass van authenticatie in de VMware Directory Service, een arbitrary file write via specifieke archive-bestanden, meerdere denial-of-service kwetsbaarheden in de Directory Service en guest RPC component, een local privilege escalation in de vpxd service script, en een failure in policy enforcement binnen de vSphere Distributed Switch.

Daarnaast zijn er kritieke heap out-of-bounds write en use-after-free kwetsbaarheden in de ESX I/O filter service, een out-of-bounds write in de XHCI USB controller, een stack-based buffer overflow in de VMkernel component, een security bypass in de host configuratie store, en een signature verification bypass in ESX en aanverwante producten.

Ook is er een denial-of-service kwetsbaarheid in de VGAuth service van VMware Tools.

Deze kwetsbaarheden kunnen leiden tot het omzeilen van beveiligingsmechanismen, het schrijven van onbevoegde bestanden, privilege escalatie, serviceonderbrekingen en mogelijk code-executie.

Oplossingen

VMware heeft updates en patches uitgebracht voor alle genoemde producten en versies om de kwetsbaarheden te verhelpen. Details en specifieke versies zijn gedocumenteerd in VMware Knowledge Base artikelen, waaronder KB463501. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39626

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-123903	9.8 CRITICAL
CVE-2026-123904	7.5 HIGH
CVE-2026-123905	7.5 HIGH
CVE-2026-123906	7.5 HIGH
CVE-2026-123907	7.5 HIGH
CVE-2026-123908	6.7 MEDIUM
CVE-2026-123909	5.2 MEDIUM
CVE-2026-123910	9.8 CRITICAL
CVE-2026-123911	9.8 CRITICAL
CVE-2026-123912	9.3 CRITICAL
CVE-2026-123913	8.2 HIGH
CVE-2026-123914	6.7 MEDIUM
CVE-2026-123915	6.3 MEDIUM
CVE-2026-123916	5.5 MEDIUM
CVE-2026-123918	5.5 MEDIUM
CVE-2026-123919	6.7 MEDIUM
CVE-2026-123920	6.7 MEDIUM
CVE-2026-123921	6.6 MEDIUM
CVE-2026-123922	4.9 MEDIUM
CVE-2026-123923	3.4 LOW
CVE-2026-123924	3.6 LOW
CVE-2026-123925	3.8 LOW
CVE-2026-123926	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-73	External Control of File Name or Path
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-347	Improper Verification of Cryptographic Signature
CWE-404	Improper Resource Shutdown or Release
CWE-416	Use After Free
CWE-787	Out-of-bounds Write

Getroffen producten

VMware
Cloud Foundation
ESXi
Fusion
Telco Cloud Infrastructure
Telco Cloud Platform
Tools

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.