



NCSC-2026-0070

Kwetsbaarheden verholpen in VMware Aria Operations

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 04-03-2026

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

CISA heeft aangegeven dat CVE-2026-22719 actief misbruikt wordt.

Feiten

Broadcom heeft kwetsbaarheden verholpen in VMware Aria Operations.

Duiding

De kwetsbaarheden omvatten een privilege-escalatie, een stored cross-site scripting (XSS) en een command injection. De privilege-escalatie kwetsbaarheid kan een aanvaller in staat stellen om verhoogde privileges te verkrijgen, wat de systeemintegriteit en toegangscontroles kan beïnvloeden. De stored XSS-kwetsbaarheid stelt aanvallers in staat om kwaadaardige scripts in de applicatie te injecteren en uit te voeren, wat kan leiden tot compromittering van gebruikerssessies of gegevensintegriteit. De command injection-kwetsbaarheid maakt het mogelijk om willekeurige commando's binnen het systeem uit te voeren, wat de systeemintegriteit of vertrouwelijkheid kan compromitteren.

UPDATE 04/03/2026: CISA heeft aangegeven dat CVE-2026-22719 actief misbruikt wordt.

Oplossingen

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

Referenties

- <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947>
- <https://www.cisa.gov/news-events/alerts/2026/03/03/cisa-adds-two-known-exploited-vulnerabilities-catalog>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-22721	6.2 MEDIUM
➤ CVE-2026-22720	8.0 HIGH

> CVE-2026-22719

8.1 HIGH

CWE's

CWE	Beschrijving
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-269	Improper Privilege Management

Getroffen producten

VMware
Aria Operations
Cloud Foundation
Telco Cloud Infrastructure
Telco Cloud Platform

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.